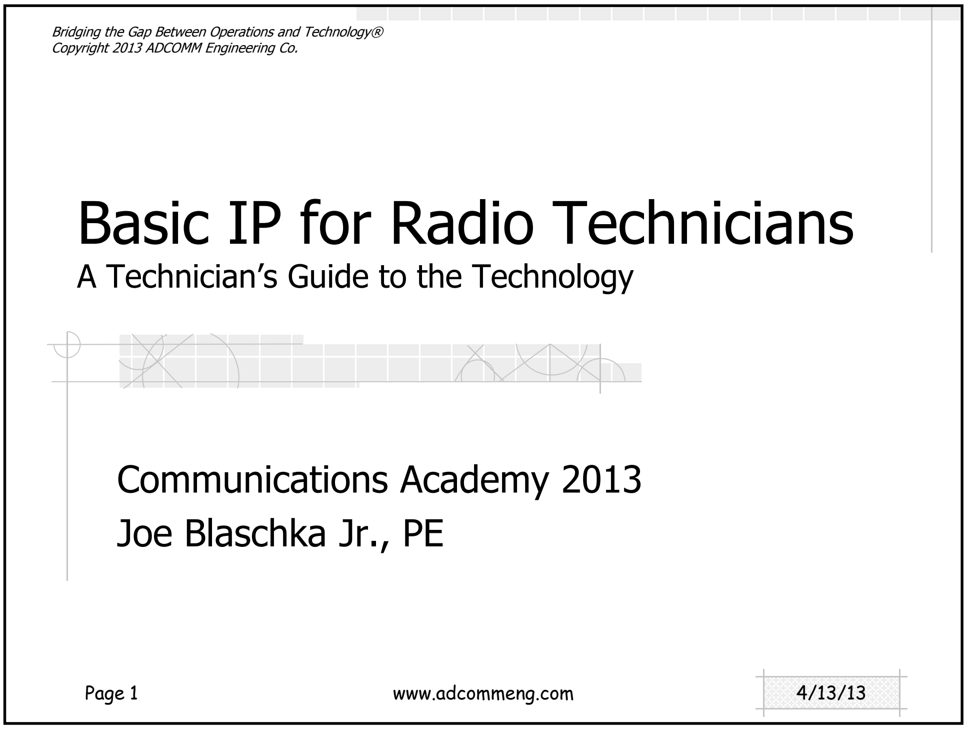
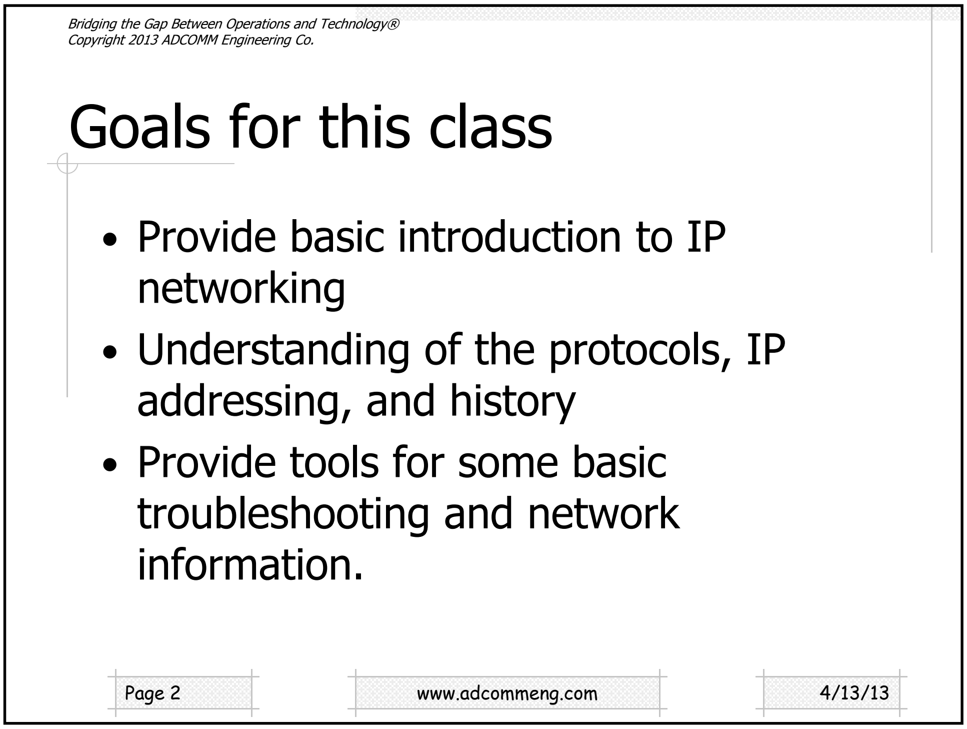


Basic IP for Radio Technicians

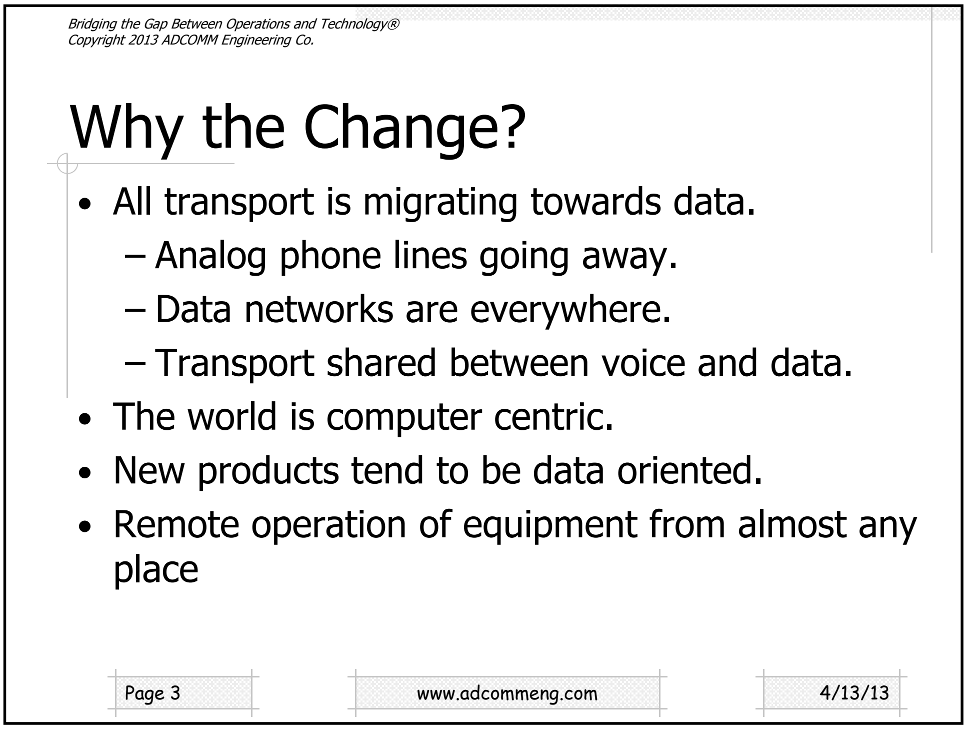
A Technician's Guide to the Technology

Communications Academy 2013
Joe Blaschka Jr., PE



Goals for this class

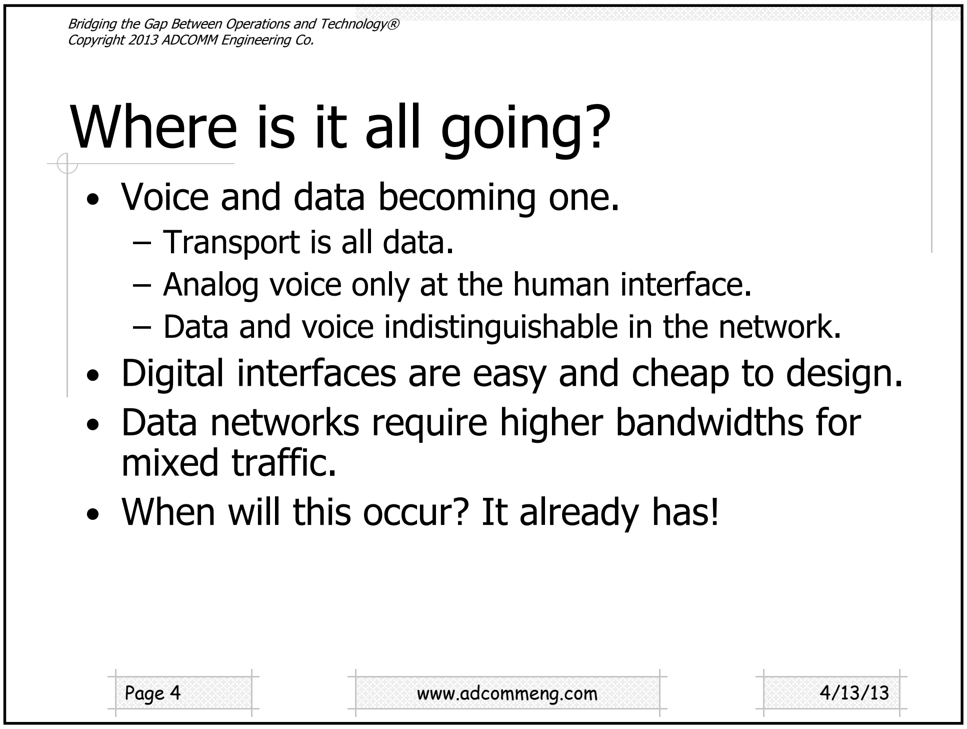
- Provide basic introduction to IP networking
- Understanding of the protocols, IP addressing, and history
- Provide tools for some basic troubleshooting and network information.



Bridging the Gap Between Operations and Technology®
Copyright 2013 ADCOMM Engineering Co.

Why the Change?

- All transport is migrating towards data.
  - Analog phone lines going away.
  - Data networks are everywhere.
  - Transport shared between voice and data.
- The world is computer centric.
- New products tend to be data oriented.
- Remote operation of equipment from almost any place



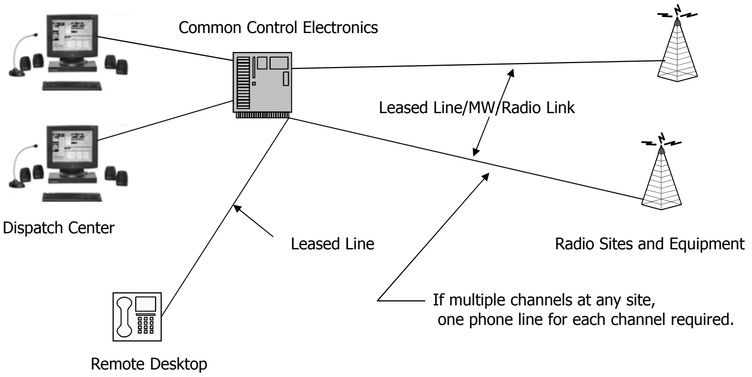
Bridging the Gap Between Operations and Technology®
Copyright 2013 ADCOMM Engineering Co.

Where is it all going?

- Voice and data becoming one.
  - Transport is all data.
  - Analog voice only at the human interface.
  - Data and voice indistinguishable in the network.
- Digital interfaces are easy and cheap to design.
- Data networks require higher bandwidths for mixed traffic.
- When will this occur? It already has!

Why IP?

- Typical radio network today



Common Control Electronics

Leased Line/MW/Radio Link

Dispatch Center

Leased Line

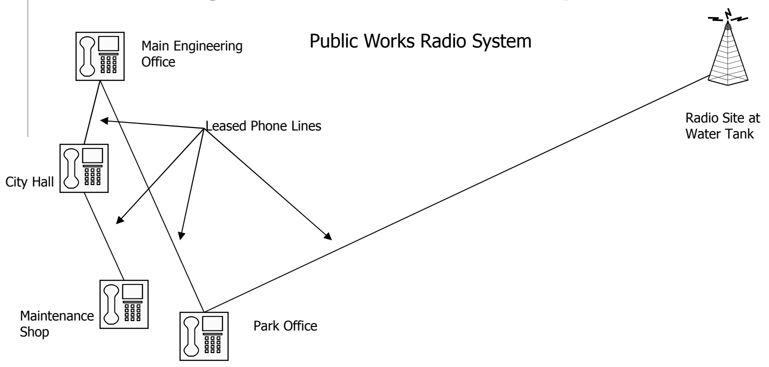
Radio Sites and Equipment

If multiple channels at any site,
one phone line for each channel required.

Remote Desktop

Why IP?

- Analog connections today.



Main Engineering Office

Public Works Radio System

Leased Phone Lines

Radio Site at Water Tank

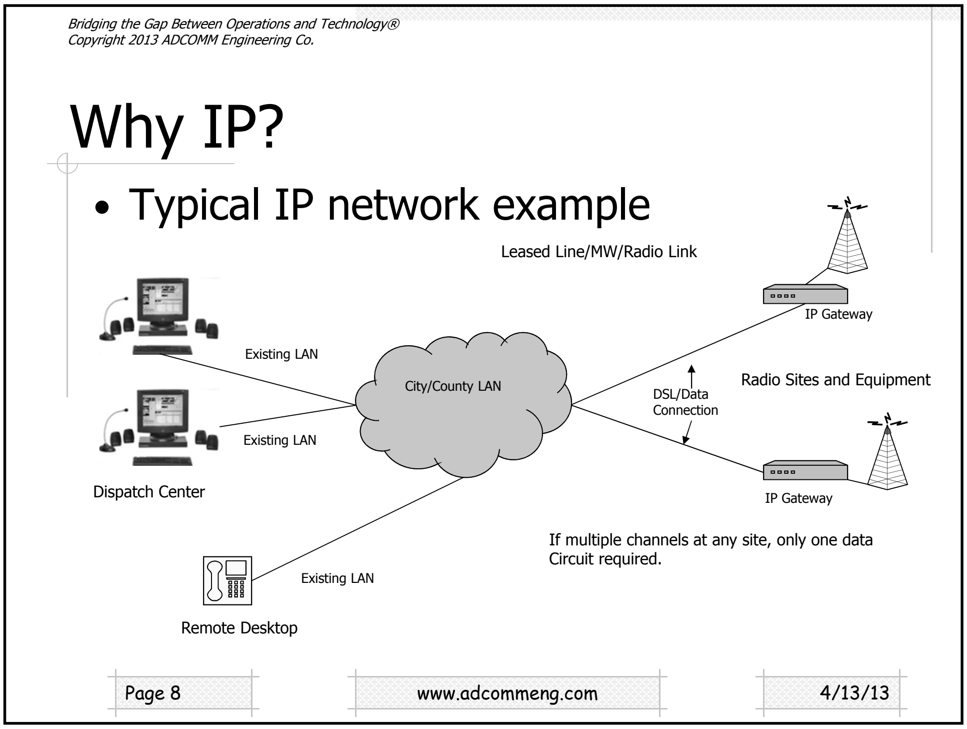
City Hall

Maintenance Shop

Park Office

Why IP?

- What do those examples have in common?
  - Use of dedicated phone lines or other interconnection method for each site/channel
  - Use of dedicated phone lines to interconnect remote console positions
  - High on-going costs for dedicated facilities
  - Loss of one connection point could cause loss of communications
  - Dedicated facilities are expensive



Why IP?

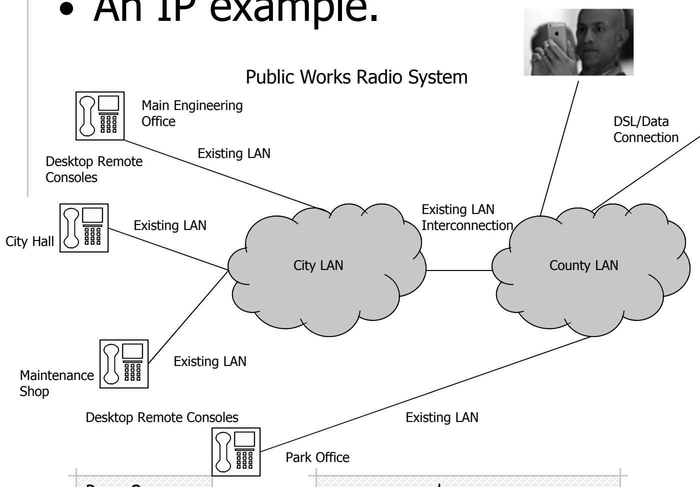
- Typical IP network example

If multiple channels at any site, only one data Circuit required.

Bridging the Gap Between Operations and Technology®
Copyright 2013 ADCOMM Engineering Co.

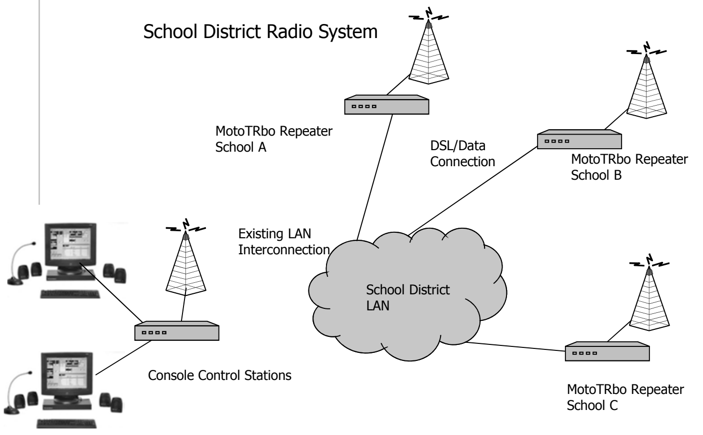
Why IP?

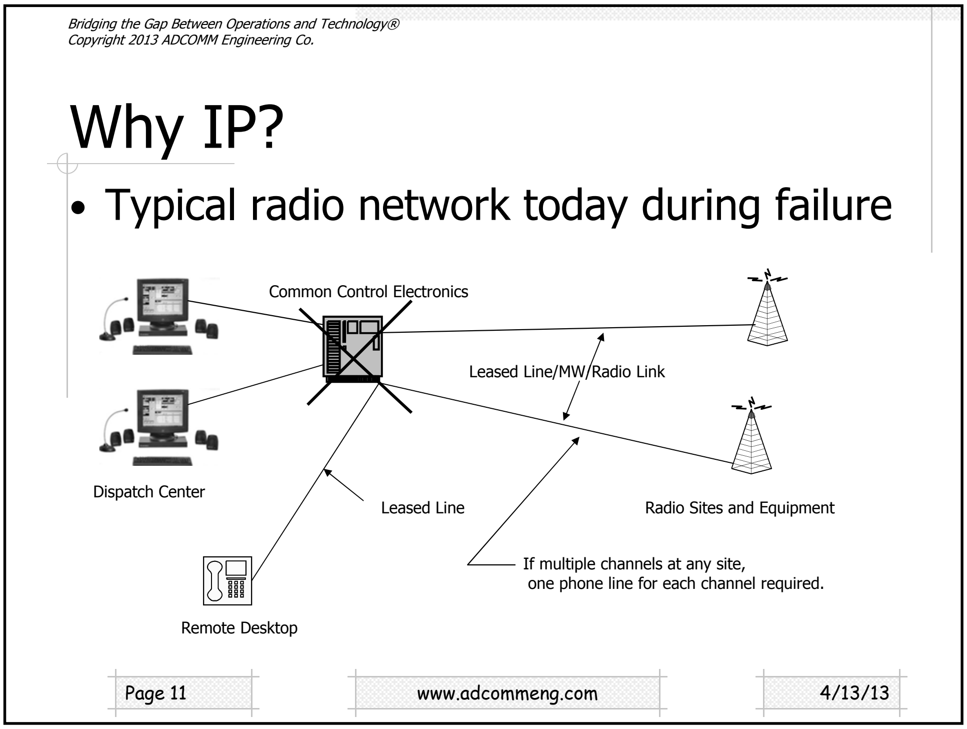
- An IP example.



Bridging the Gap Between Operations and Technology®
Copyright 2013 ADCOMM Engineering Co.

IP Network Example


School District Radio System
MotoTRbo Repeater School A
DSL/Data Connection
MotoTRbo Repeater School B
Existing LAN Interconnection
School District LAN
Console Control Stations
MotoTRbo Repeater School C



Bridging the Gap Between Operations and Technology®

Why IP?

- Typical radio network today during failure

Common Control Electronics

Leased Line/MW/Radio Link

Dispatch Center

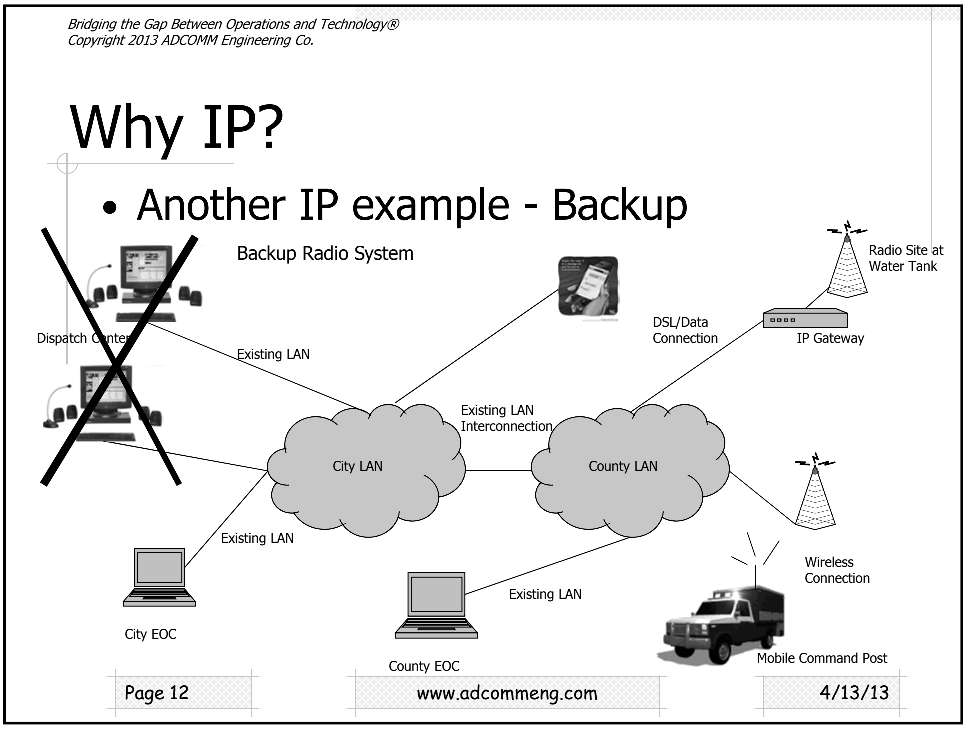
Leased Line

Radio Sites and Equipment

If multiple channels at any site,
one phone line for each channel required.

Remote Desktop

Page 11 www.adcommeng.com 4/13/13



Bridging the Gap Between Operations and Technology®

Why IP?

- Another IP example - Backup

Backup Radio System

Radio Site at
Water Tank

Dispatch Center

DSL/Data
Connection

IP Gateway

Existing LAN

Existing LAN
Interconnection

City LAN

County LAN

Existing LAN

Wireless
Connection

Existing LAN

City EOC

County EOC

Mobile Command Post

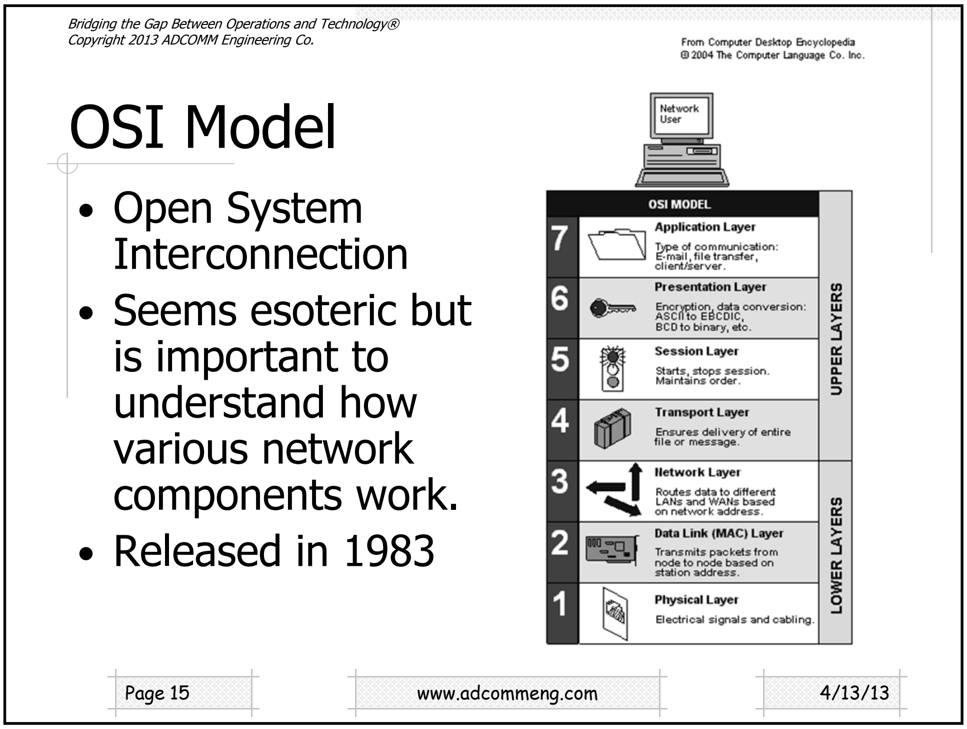
Page 12 www.adcommeng.com 4/13/13

How can IP be used for radio?

- It is a method of interconnecting consoles, radios, telephones, and other devices
- It is not transmitted over-the-air to the user radios
- IP ≠ P25
- Uses standard Internet Protocols (IP)
  - TCP/IP – Most reliable format because provides guaranteed delivery but not generally used for voice because of bandwidth
  - UDP/IP – Uses less bandwidth but may be less reliable because no guaranteed delivery
  - Uses many of the standards and protocols available in most data networks but not necessarily allowed by the network manager

The Promise of IP

- Reduces costs because existing data networks can be used
- Easy to use, interconnects many different brands of equipment
- Control consoles can be located anywhere there is a data network and a simple laptop can be used
- Reduces costs because standard computer hardware can be used
- Great for disaster recovery and back up because IP data networks are often more resilient than voice or dedicated facilities
- Reduces costs because one data circuit can handle multiple base stations
- Interconnects many different kinds of equipment such as cell phones, 2-way radio, Internet Phones, VoIP phones, etc.
- Plug and Play



OSI Model

- Open System Interconnection
- Seems esoteric but is important to understand how various network components work.
- Released in 1983

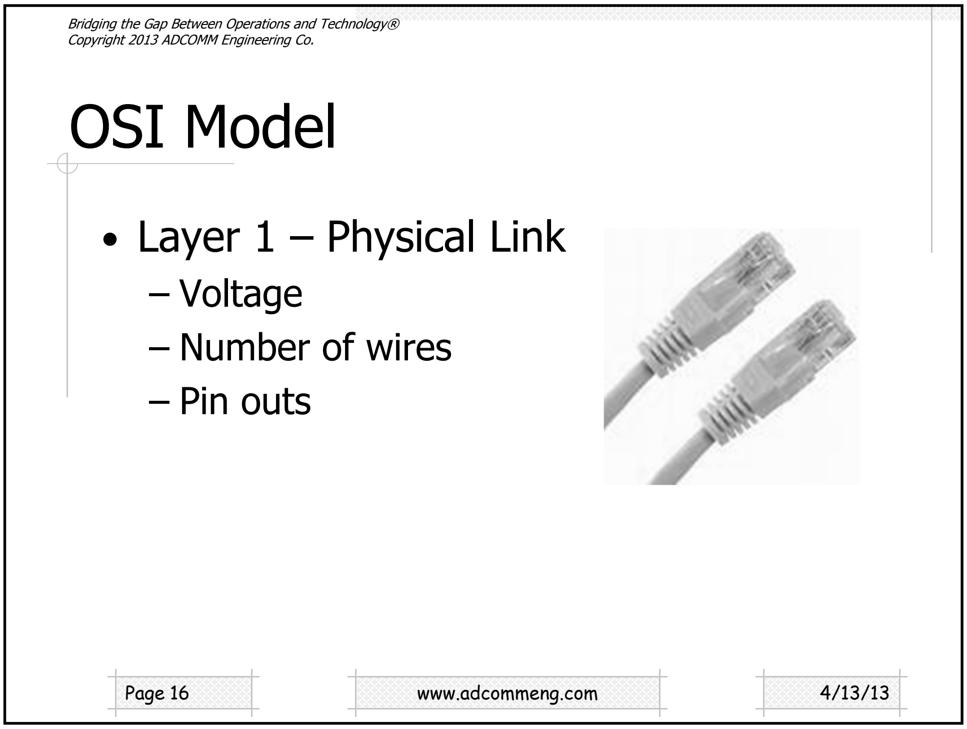
From Computer Desktop Encyclopedia
© 2004 The Computer Language Co. Inc.

Network User

OSI MODEL

7 **Application Layer** Type of communication: E-mail, file transfer, client/server.
6 **Presentation Layer** Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.
5 **Session Layer** Starts, stops session. Maintains order.
4 **Transport Layer** Ensures delivery of entire file or message.
3 **Network Layer** Routes data to different LANs and WANs based on network address.
2 **Data Link (MAC) Layer** Transmits packets from node to node based on station address.
1 **Physical Layer** Electrical signals and cabling.

UPPER LAYERS
LOWER LAYERS



OSI Model

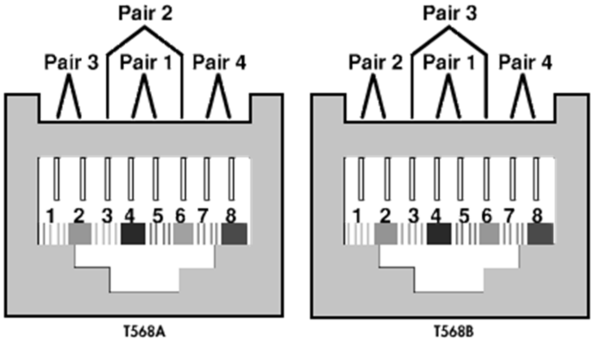
- Layer 1 – Physical Link
  - Voltage
  - Number of wires
  - Pin outs

Layer 1 Wiring

- Layer 1 Wiring standards
- Connector 8P8C (not really RJ45)
  - TIA 568A
    - Recommended for general use
    - Compatible with T1 USOC RJ-48C
    - Recommended for home networks TIA 570
    - Compatible with voice telephone line RJ11 type connections
  - TIA 568B
    - Most common in commercial applications
    - Legacy "Bell System" wiring (Merlin systems)

Layer 1 Wiring

- TIA 568 Pin outs

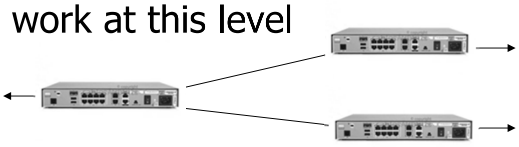


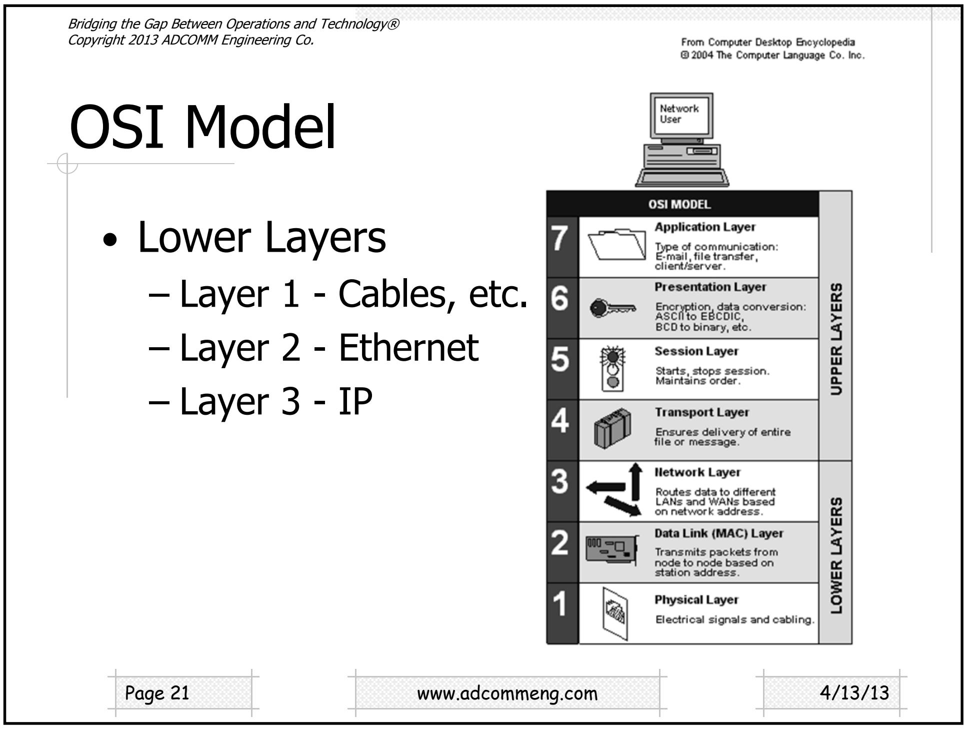
OSI Model

- Layer 2 – Data Link
  - Media Access Control (MAC) Addresses
  - Ethernet, Token Ring, Frame Relay, ATM
  - Data “Switches” usually work at this level
  - LAN Cards – Usually Layer 2 depending on card
  - Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA-CD)

OSI Model

- Layer 3 – Network Layer
  - Higher level addressing
  - Handles communications between network switching points.
  - Routers generally operate at this level
  - IP, SNA, Apple Talk
  - IP addresses work at this level





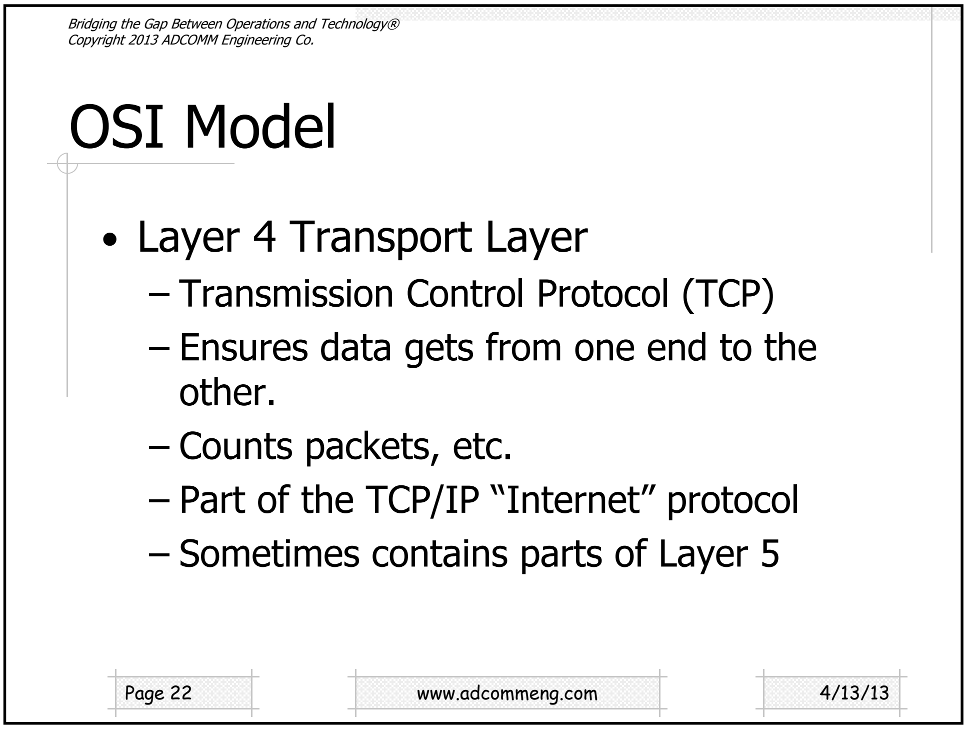
Bridging the Gap Between Operations and Technology®
Copyright 2013 ADCOMM Engineering Co.

OSI Model

- Lower Layers
  - Layer 1 - Cables, etc.
  - Layer 2 - Ethernet
  - Layer 3 - IP

From Computer Desktop Encyclopedia
© 2004 The Computer Language Co. Inc.
Network User
OSI MODEL
7 Application Layer
Type of communication: E-mail, file transfer, client/server.
6 Presentation Layer
Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.
5 Session Layer
Starts, stops session. Maintains order.
4 Transport Layer
Ensures delivery of entire file or message.
3 Network Layer
Routes data to different LANs and WANs based on network address.
2 Data Link (MAC) Layer
Transmits packets from node to node based on station address.
1 Physical Layer
Electrical signals and cabling.
UPPER LAYERS
LOWER LAYERS

Page 21 www.adcommeng.com 4/13/13



Bridging the Gap Between Operations and Technology®
Copyright 2013 ADCOMM Engineering Co.

OSI Model

- Layer 4 Transport Layer
  - Transmission Control Protocol (TCP)
  - Ensures data gets from one end to the other.
  - Counts packets, etc.
  - Part of the TCP/IP “Internet” protocol
  - Sometimes contains parts of Layer 5

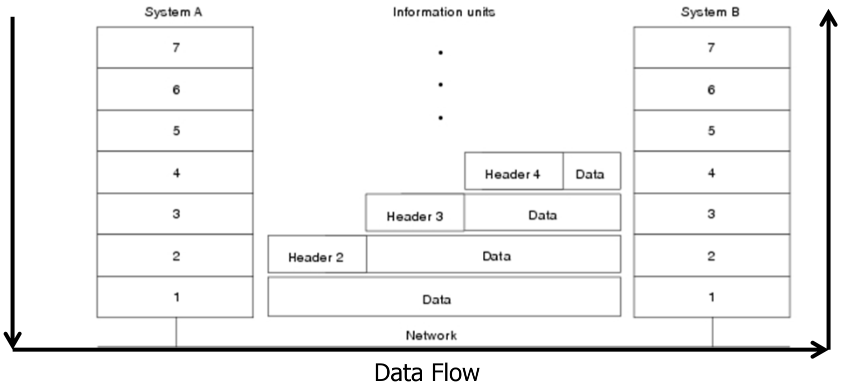
Page 22 www.adcommeng.com 4/13/13

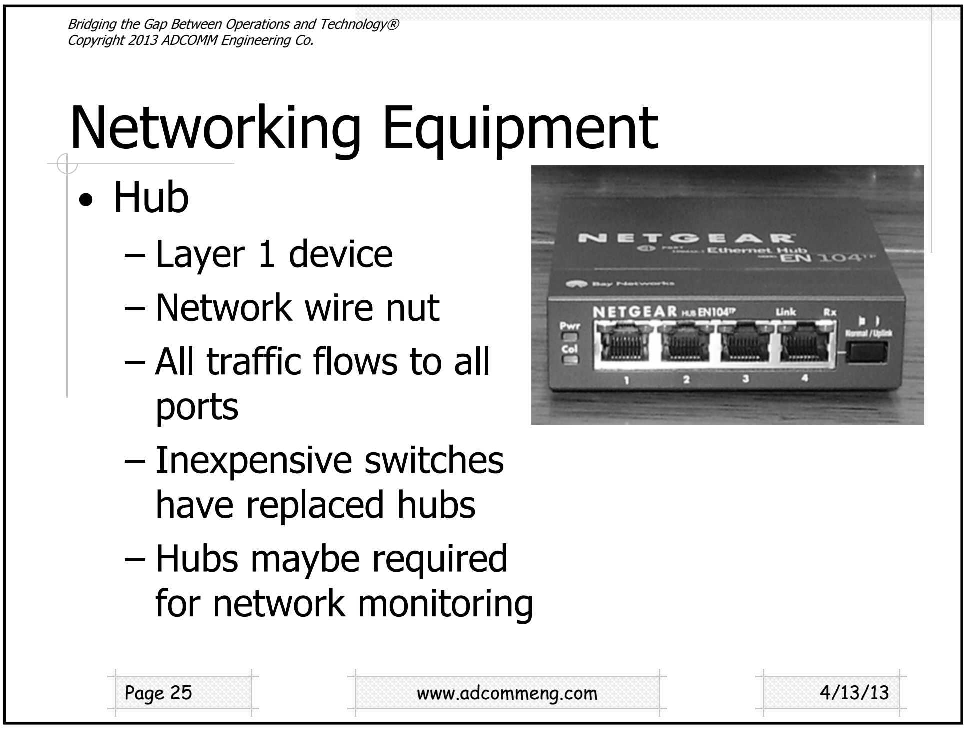
OSI Model

- Layer 5 – Session Layer
  - Manages two-way or one-way transmission
  - Provides communications coordination
  - Often incorporated in Layer 4
- Layer 6 – Presentation Layer
  - Use has changed over time
  - Generally used for encryption now.
- Layer 7 – Application Layer
  - Used to manage the applications such as file transfers, etc.
- Layers 5, 6, and 7 are often merged together in the operating system or applications in modern computers.

Network Data Flow

- Data flows through the OSI model elements.



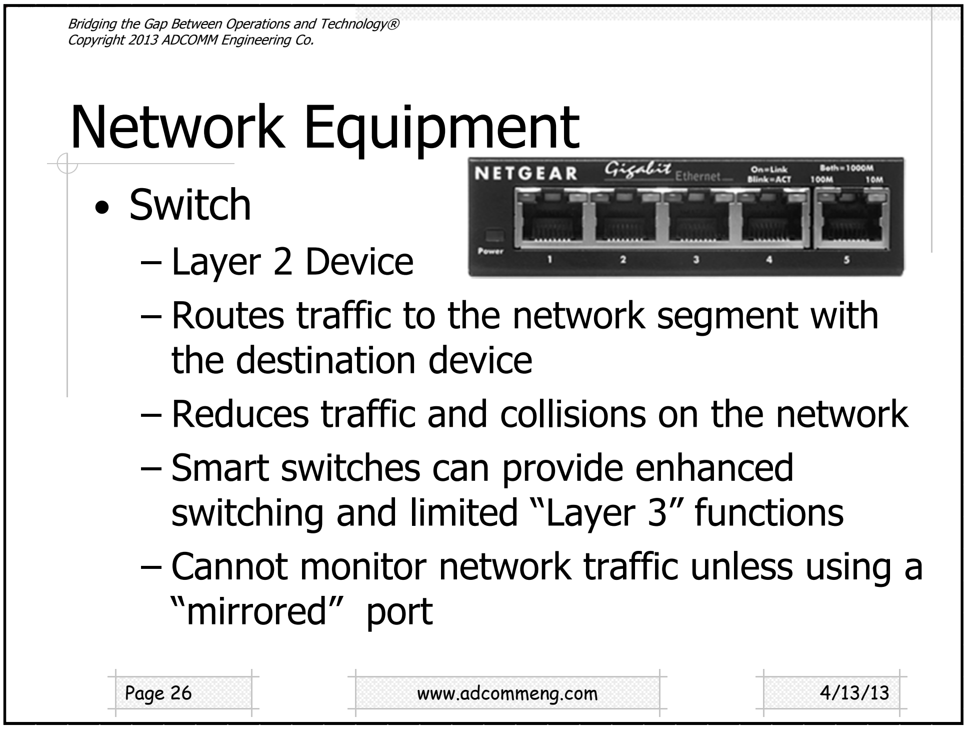


Bridging the Gap Between Operations and Technology®
Copyright 2013 ADCOMM Engineering Co.

Networking Equipment

- Hub
  - Layer 1 device
  - Network wire nut
  - All traffic flows to all ports
  - Inexpensive switches have replaced hubs
  - Hubs maybe required for network monitoring

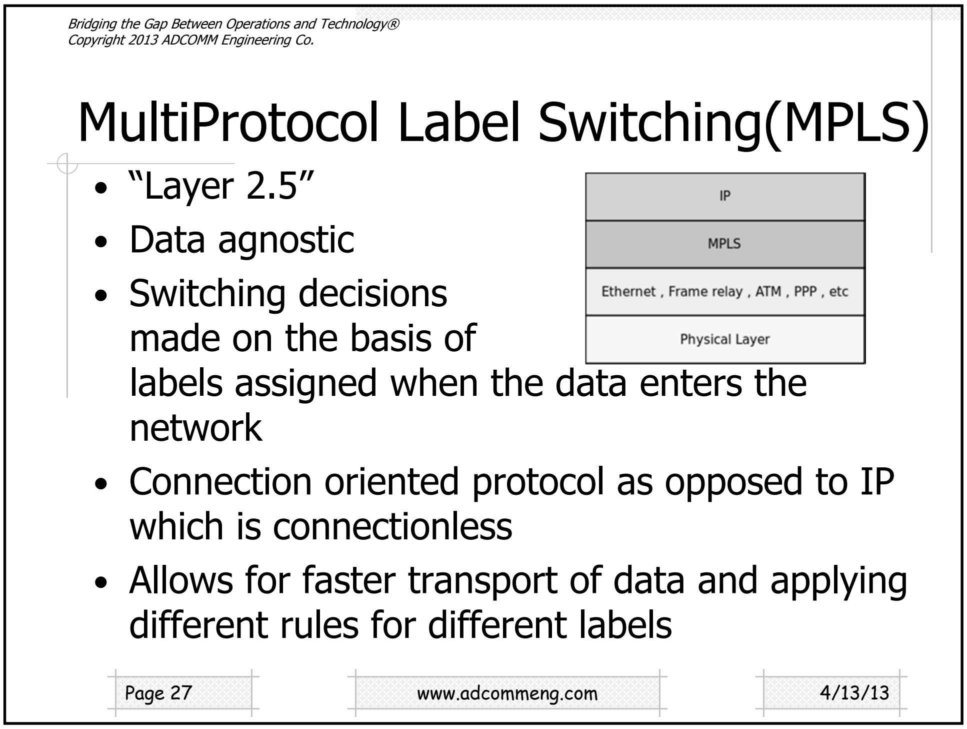
NETGEAR
Ethernet Hub
EN 104TP
Bay Networks
NETGEAR HUB EN104TP
Link
Rx
Pwr
Col
Normal / Uplink
1
2
3
4



Bridging the Gap Between Operations and Technology®
Copyright 2013 ADCOMM Engineering Co.

Network Equipment

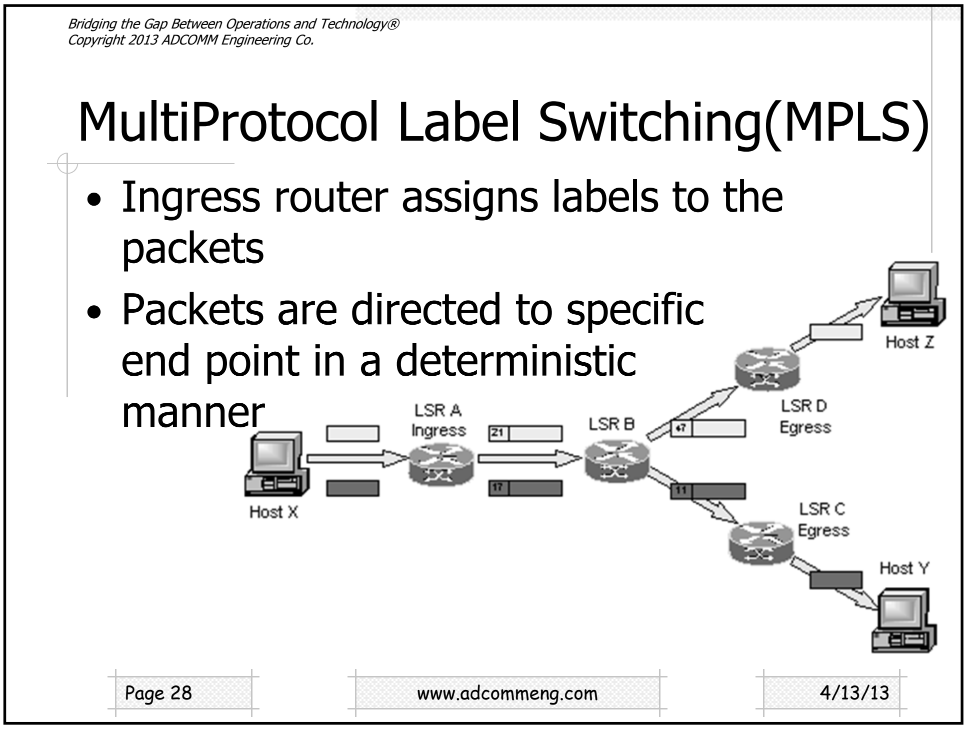
- Switch
  - Layer 2 Device
  - Routes traffic to the network segment with the destination device
  - Reduces traffic and collisions on the network
  - Smart switches can provide enhanced switching and limited "Layer 3" functions
  - Cannot monitor network traffic unless using a "mirrored" port



Bridging the Gap Between Operations and Technology®

MultiProtocol Label Switching(MPLS)

- "Layer 2.5"
- Data agnostic
- Switching decisions made on the basis of labels assigned when the data enters the network
- Connection oriented protocol as opposed to IP which is connectionless
- Allows for faster transport of data and applying different rules for different labels



Bridging the Gap Between Operations and Technology®

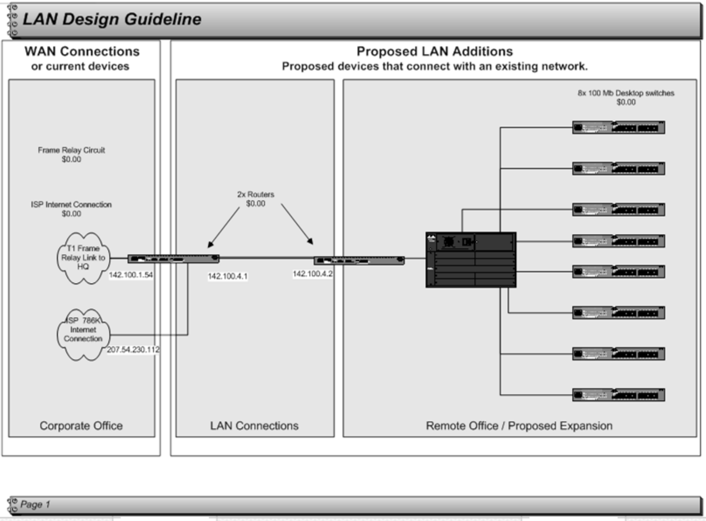
MultiProtocol Label Switching(MPLS)

- Ingress router assigns labels to the packets
- Packets are directed to specific end point in a deterministic manner

Networking Equipment

- Routers
  - Layer 3 Device
  - Connects one network to another
  - Usually provides transport conversion
  - Makes “intelligent” decisions about how to route data

Putting it all together

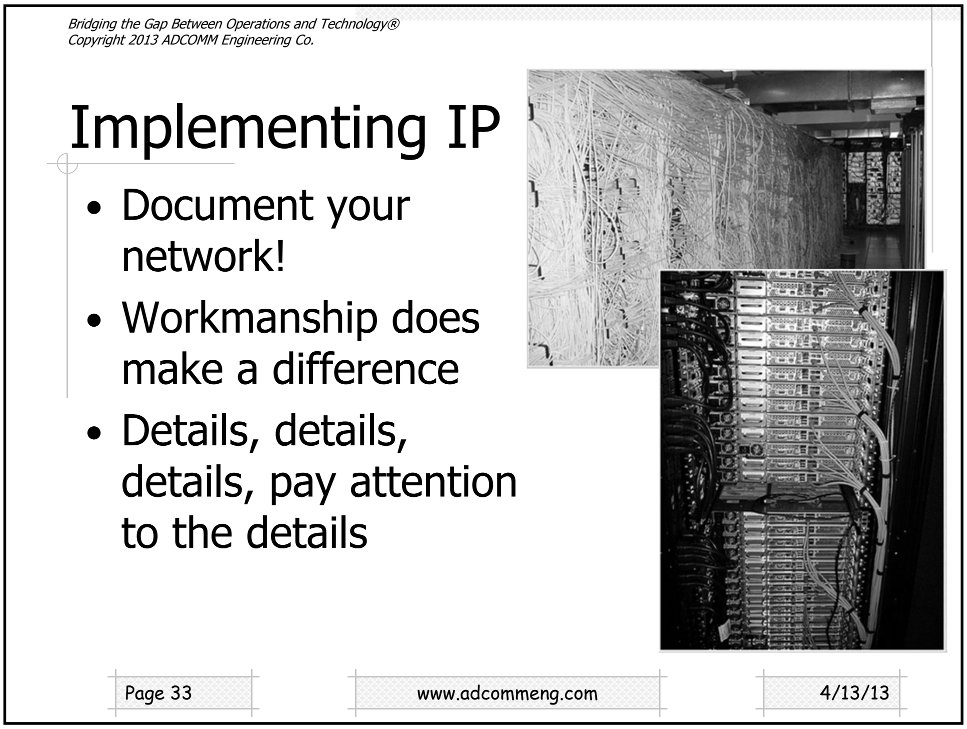


Initial Considerations

- Shared or dedicated network
- Shared network should support
  - Multicast – Transmits to multiple points simultaneously
  - Bandwidth – Depends on vocoding assume 50k per voice channel worst case
  - Fixed IP addresses
  - Dedicated bandwidth or Quality of Service
  - Virtual LAN's do not guarantee bandwidth
  - Delay must be controlled
  - Router/Firewall programming control
  - Security and virus protection

Technical Details

- Data Networking
  - Common use:
    - TCP/IP for control signals – More reliable
    - UDP/IP for voice data – Less bandwidth
    - Multicast – Routing data to multiple points
    - Fixed IP addresses
    - Be careful with any network assumptions as different vendors have implemented network interfaces differently.
  - Quality of service is generally required to ensure delivery of audio packets. (Remember they are UDP/IP.)
  - Multiple ports may need to be opened in firewalls, etc. for proper operation.
  - Virtual LANs do not guarantee bandwidth.
  - Network security must be managed.

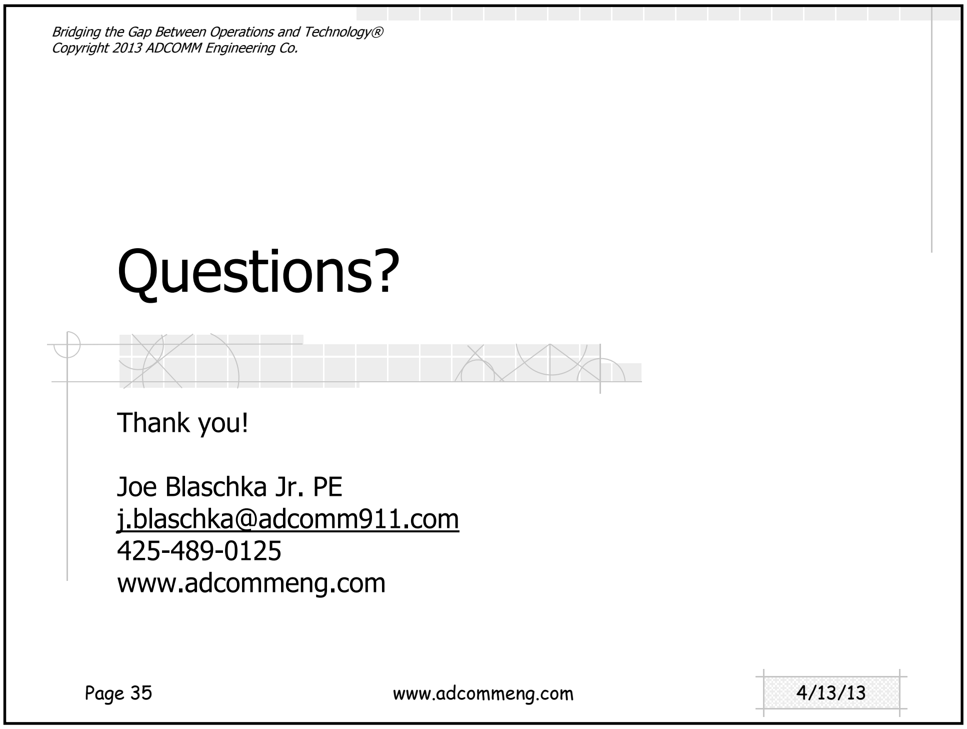


Implementing IP

- Document your network!
- Workmanship does make a difference
- Details, details, details, pay attention to the details

IP – The Future is Now

- Good news
  - Can be a very cost effective solution in some situations
  - If limitations are not a problem, costs can be reduced
  - This technology will eventually become the dominate method for radio system interconnection because most communications are moving to an IP type network
  - Improvements in the interfaces are being made all the time
  - Some issues are resolved if implemented on a dedicated data network but that raises costs



Bridging the Gap Between Operations and Technology®

Questions?

Thank you!

Joe Blaschka Jr. PE
j.blaschka@adcomm911.com
425-489-0125
www.adcommeng.com

IP Network Basics

Communications Academy 2013
Dave Magnenat

Agenda

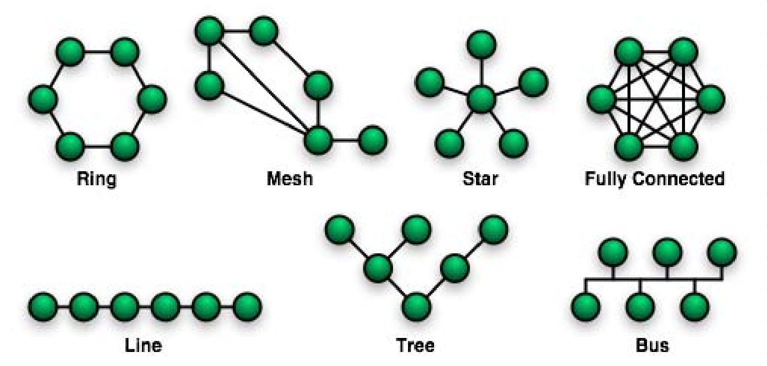
- Network characteristics
- Internetworking Protocol
- IP addressing & devices

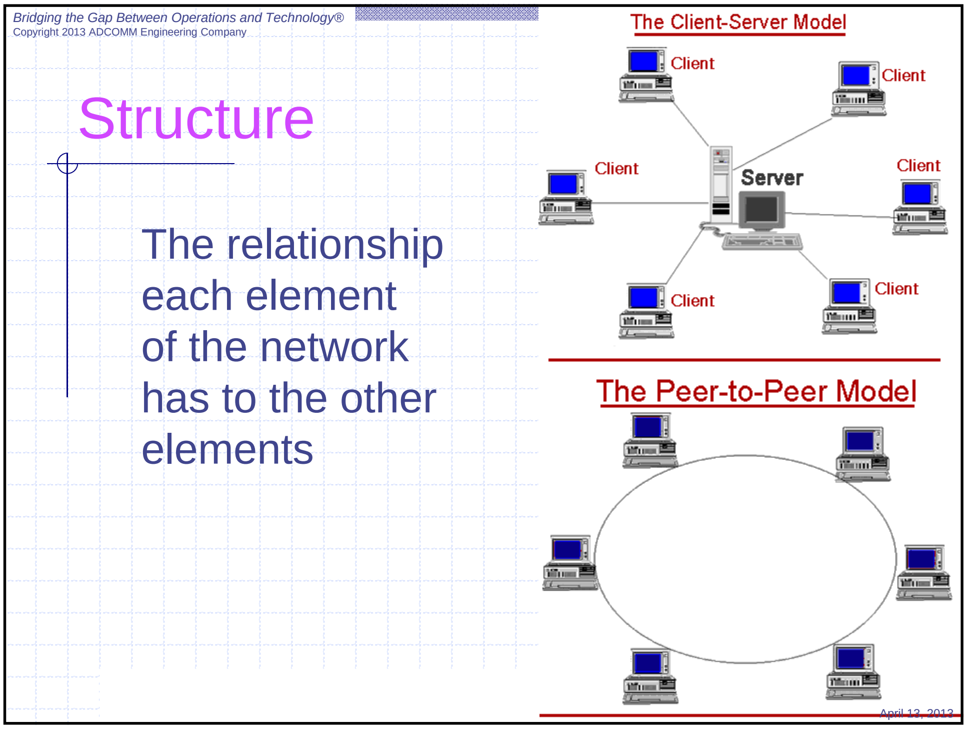
Network Characteristics

- Topology – what shape it is
- Structure – relationship between members
- Switching – pathways for moving information
- Protocol – rules for communication

Networks

- Topologies



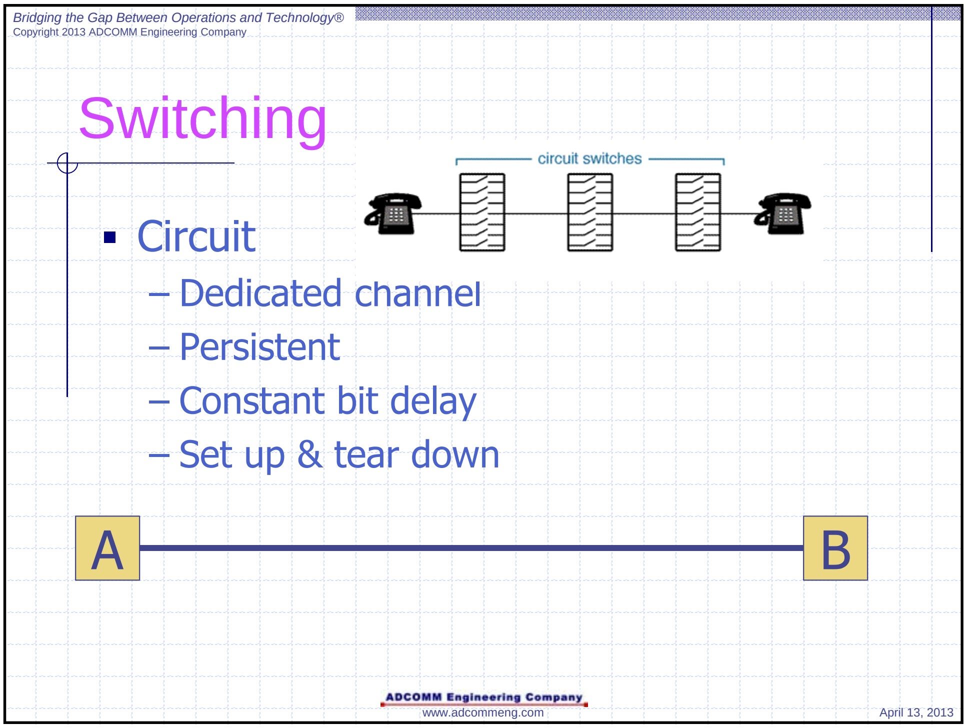


Bridging the Gap Between Operations and Technology®

Structure

The relationship each element of the network has to the other elements

April 13, 2013



Bridging the Gap Between Operations and Technology®

Switching

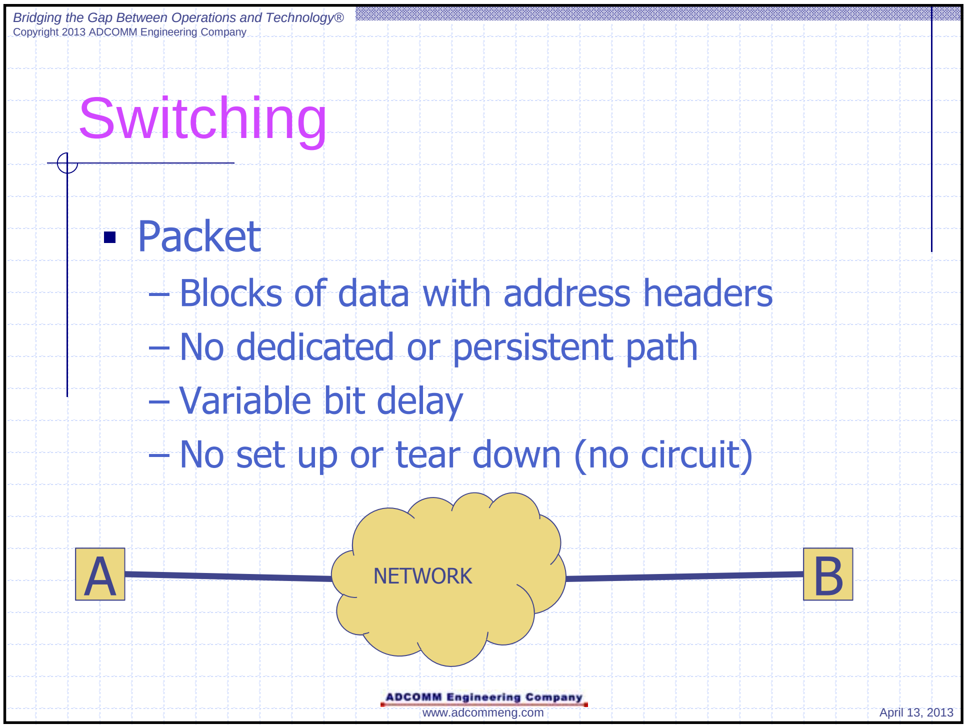
- Circuit
  - – Dedicated channel
  - – Persistent
  - – Constant bit delay
  - – Set up & tear down

ADCOMM Engineering Company
www.adcommeng.com

April 13, 2013

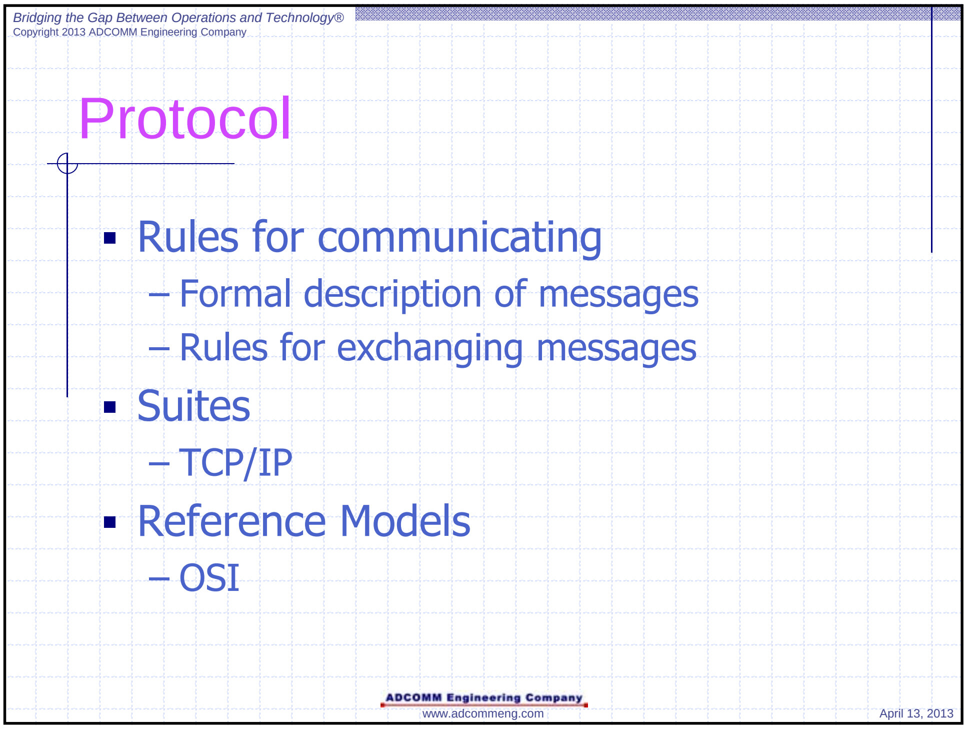
Switching

- Circuit
  - "Nailed up" "Copper" "Leased Line" "Point to Point"
- Virtual circuit
  - Setup before transmission
  - Persistent
  - Really connection-oriented packet switching



Switching

- Packet
  - Blocks of data with address headers
  - No dedicated or persistent path
  - Variable bit delay
  - No set up or tear down (no circuit)

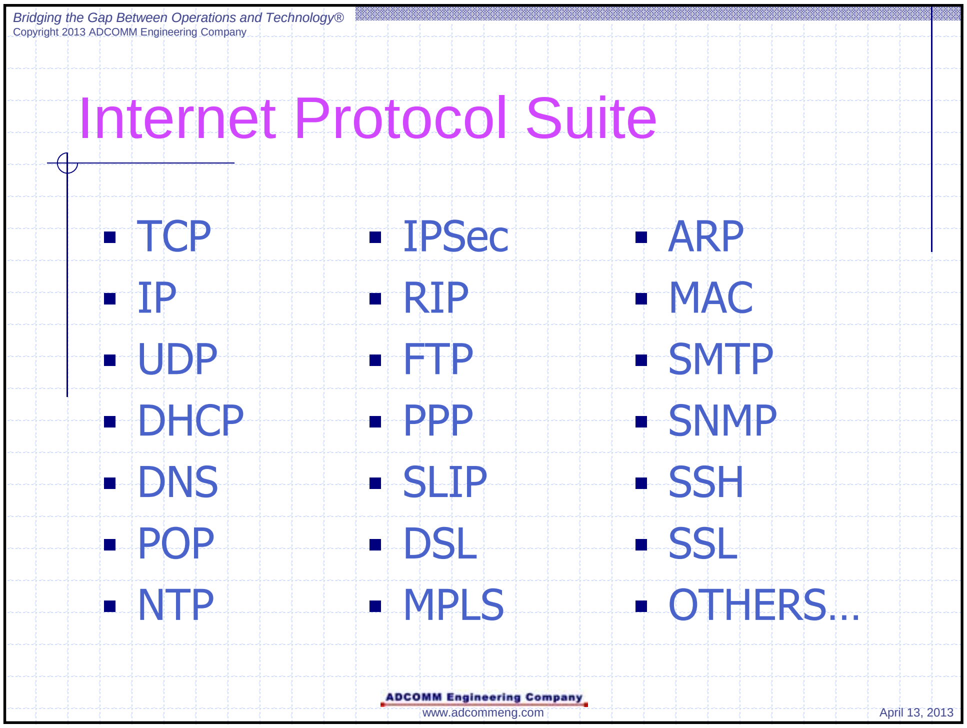


Bridging the Gap Between Operations and Technology®

Protocol

- Rules for communicating
  - Formal description of messages
  - Rules for exchanging messages
- Suites
  - TCP/IP
- Reference Models
  - OSI

ADCOMM Engineering Company
www.adcommeng.com
April 13, 2013



Bridging the Gap Between Operations and Technology®

Internet Protocol Suite

- TCP
- IP
- UDP
- DHCP
- DNS
- POP
- NTP
- IPSec
- RIP
- FTP
- PPP
- SLIP
- DSL
- MPLS
- ARP
- MAC
- SMTP
- SNMP
- SSH
- SSL
- OTHERS…

ADCOMM Engineering Company
www.adcommeng.com
April 13, 2013

Internet Protocol Suite

- DNS – Domain Name Service
- POP – Post Office Protocol (POP3)
- MPLS – Multiprotocol Label Switching
- ARP – Address Resolution Protocol
- SMTP – Simple Mail Transfer Protocol
- SNMP – Simple Network Management Protocol
- SSH – Secure Shell
- SSL – Secure Socket Layer
- HTTP & HTTPS – Hypertext Transfer Protocol (Secure)

TCP

- Reliable
- Provides error free reassembly of IP packets & related control
- Connection-oriented
- Layer 4 protocol

Bridging the Gap Between Operations and Technology®

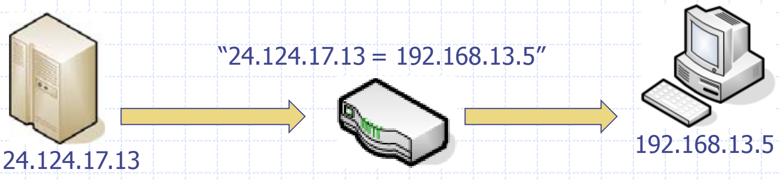
UDP

- "Best Effort" – unreliable
- No error correction
- Great for streaming media, VoIP
- Connection-less oriented
- Layer 4 protocol

Bridging the Gap Between Operations and Technology®

NAT

- Network Address Translation
- Attempt to resolve IPv4 address exhaustion
- Changes IP and other data in packet as it passes through router



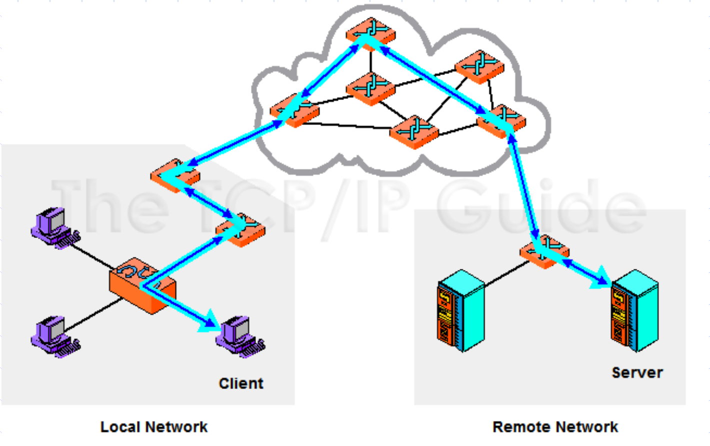
Bridging the Gap Between Operations and Technology®

DHCP

- Dynamic Host Configuration Protocol
- "Obtain an IP address automatically" in Windows

Bridging the Gap Between Operations and Technology®

What is IP?

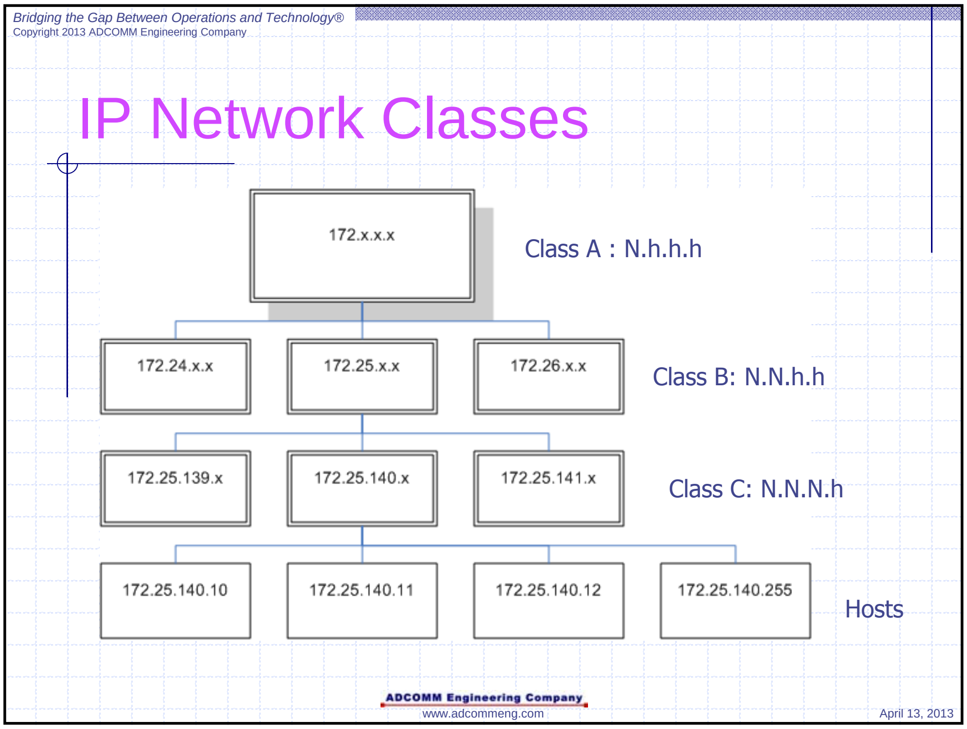


What is IP ?

- A numbering system used to describe networked devices uniquely within a domain
- (Version 4) 32 bit, divided into 4 "octets"
  - 194.25.140.12
- Describes "Networks" and "Hosts"

IP Addresses - Classful

- Network and Host:
  - N.N.N.h (Class C address)
    - 194.25.140.(0-255)
  - N.N.h.h (Class B address)
    - 129.25.(0-255).(0-255)
  - N.h.h.h (Class A address)
    - 116.(0-255).(0-255).(0-255)



Bridging the Gap Between Operations and Technology®

IP Network Classes

172.x.x.x

Class A : N.h.h.h

172.24.x.x
172.25.x.x
172.26.x.x

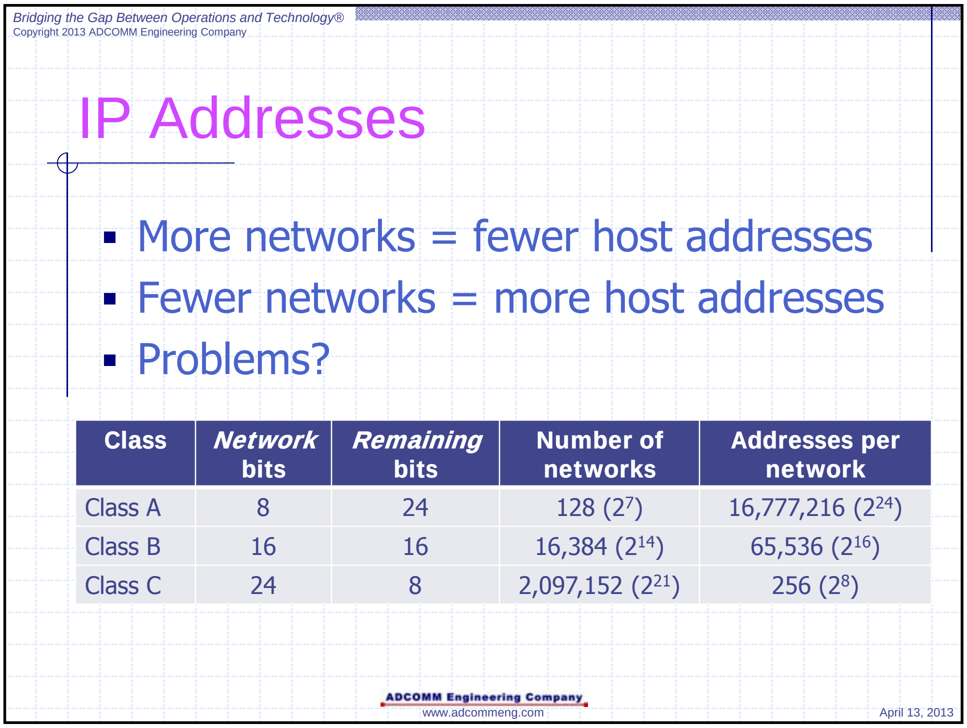
Class B: N.N.h.h

172.25.139.x
172.25.140.x
172.25.141.x

Class C: N.N.N.h

172.25.140.10
172.25.140.11
172.25.140.12
172.25.140.255

Hosts



Bridging the Gap Between Operations and Technology®

IP Addresses

- More networks = fewer host addresses
- Fewer networks = more host addresses
- Problems?

Class	*Network* bits	*Remaining* bits	Number of networks	Addresses per network
Class A	8	24	128 (2^7)	16,777,216 (2^{24})
Class B	16	16	16,384 (2^{14})	65,536 (2^{16})
Class C	24	8	2,097,152 (2^{21})	256 (2^8)

IP Addresses

- Classless Inter Domain Routing (CIDR)
  - Break out addressing anywhere
  - More flexibility
  - No huge jump in N vs h
- Combines IP address & Subnet Mask
- 192.13.10.0/24 indicates “range of network addresses from 192.13.10.0 through 192.13.10.255”

IP Versions

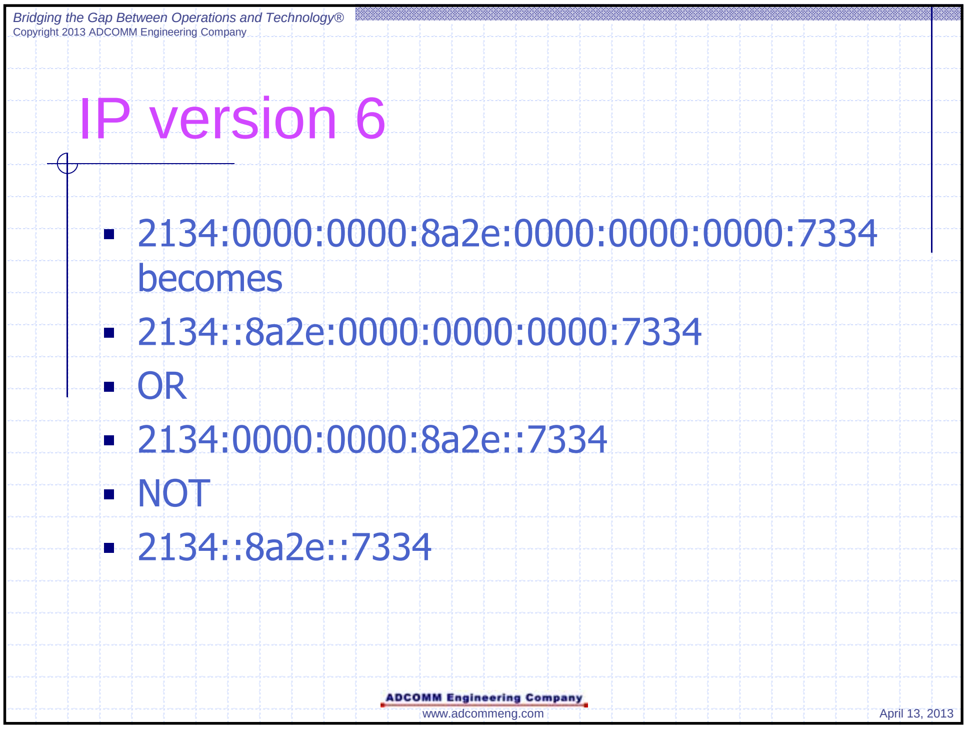
- IPv4
  - 4 billion address (4.3 x 10^9)
  - 32 bit addressing (4 octets)
- IPv6
  - 128 bit addressing (8 hextets)
  - 340 undecillion, or 3.4×10^38 addresses

IP Version 6

- 8 groups of 4 hexadecimal digits separated by colons
- 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Abbreviation rules:
  - – Drop leading 0's in a 16 bit digit
  - – Single consecutive 0 groups replaced by ::
  - – Can't use :: twice in one address

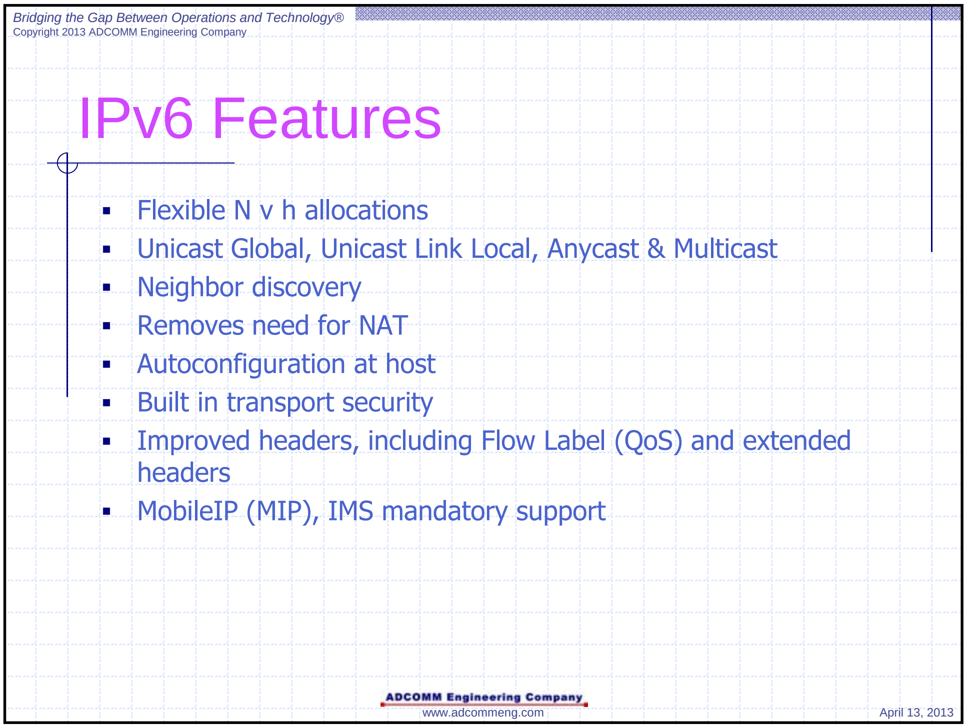
IP Version 6

- 2001:0db8:85a3:0000:0000:8a2e:0370:7334 becomes
- 2001:db8:85a3:0000:0000:8a2e:370:7334 (drop leading 0's) or
- 2001:0db8:85a3::8a2e:0370:7334 (groups of 0's replaced by colons)
- 2001:db8:85a3::8a2e:370:7334 (both)



IP version 6

- 2134:0000:0000:8a2e:0000:0000:0000:7334 becomes
- 2134::8a2e:0000:0000:0000:7334
- OR
- 2134:0000:0000:8a2e::7334
- NOT
- 2134::8a2e::7334



IPv6 Features

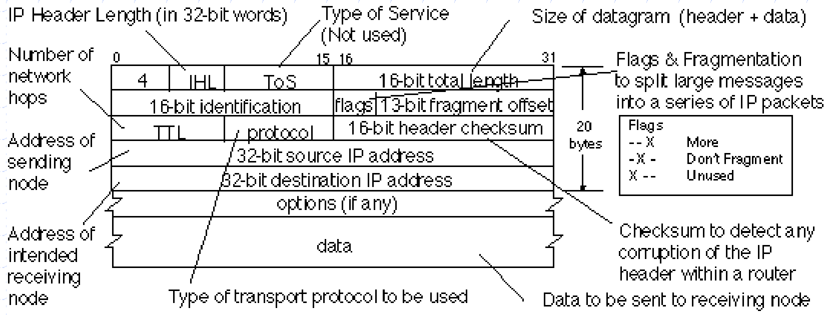
- Flexible N v h allocations
- Unicast Global, Unicast Link Local, Anycast & Multicast
- Neighbor discovery
- Removes need for NAT
- Autoconfiguration at host
- Built in transport security
- Improved headers, including Flow Label (QoS) and extended headers
- MobileIP (MIP), IMS mandatory support

IPv4 to IPv6 Transitions

- Dual Stack: hardware runs IPv4 & IPv6 both
- Tunneling: One protocol goes inside the other
- Network Address Translation – Protocol Translation (NAT-PT): translates one to the other

---

IP Packet Header


IP Header Length (in 32-bit words)
Type of Service (Not used)
Size of datagram (header + data)
Number of network hops
0
15
16
31
4
IHL
ToS
16-bit total length
16-bit identification
flags
13-bit fragment offset
TTL
protocol
16-bit header checksum
32-bit source IP address
32-bit destination IP address
options (if any)
data
20 bytes
Flags & Fragmentation to split large messages into a series of IP packets
Flags
-- X More
-X - Don't Fragment
X -- Unused
Address of sending node
Address of intended receiving node
Checksum to detect any corruption of the IP header within a router
Type of transport protocol to be used
Data to be sent to receiving node

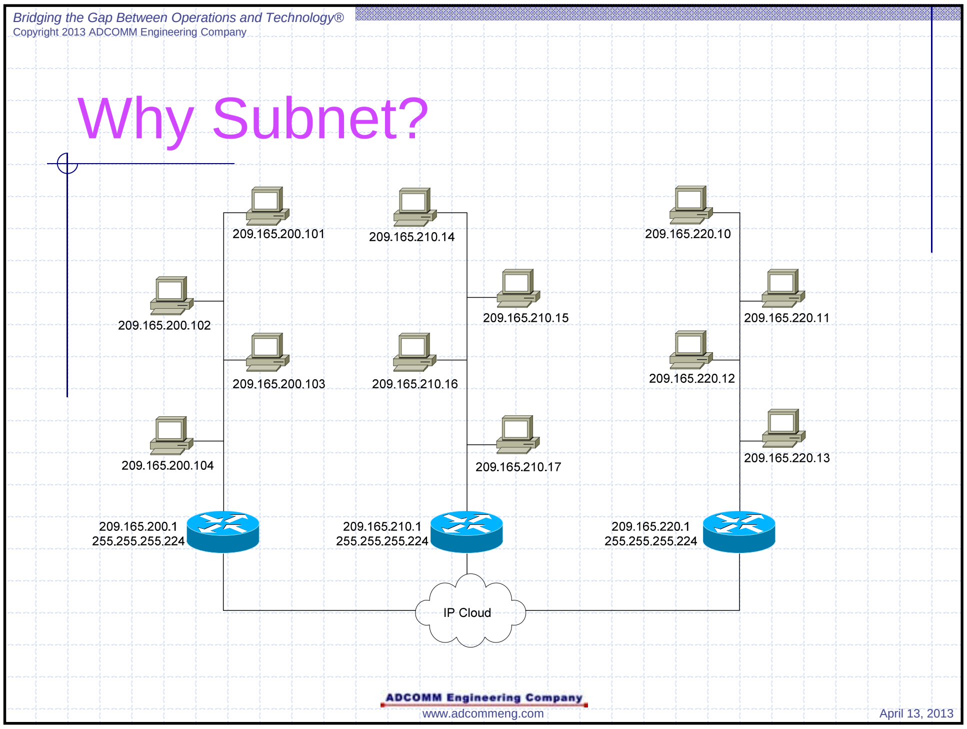
Class breakdown

Class	Leading bits	Start	End	CIDR suffix	Default subnet mask
Class A	0	0.0.0.0	127.255.255.255	/8	255.0.0.0
Class B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Class C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
Class D (multicast)	1110	224.0.0.0	239.255.255.255	/4	not defined
Class E (reserved)	1111	240.0.0.0	255.255.255.255	/4	not defined

---

Subnetting: Why you care

- Subnets define what is IN your network and what is OUT
- Addresses in network are handled locally
- Addresses out of network are sent to a “gateway”
- Common place to screw up network

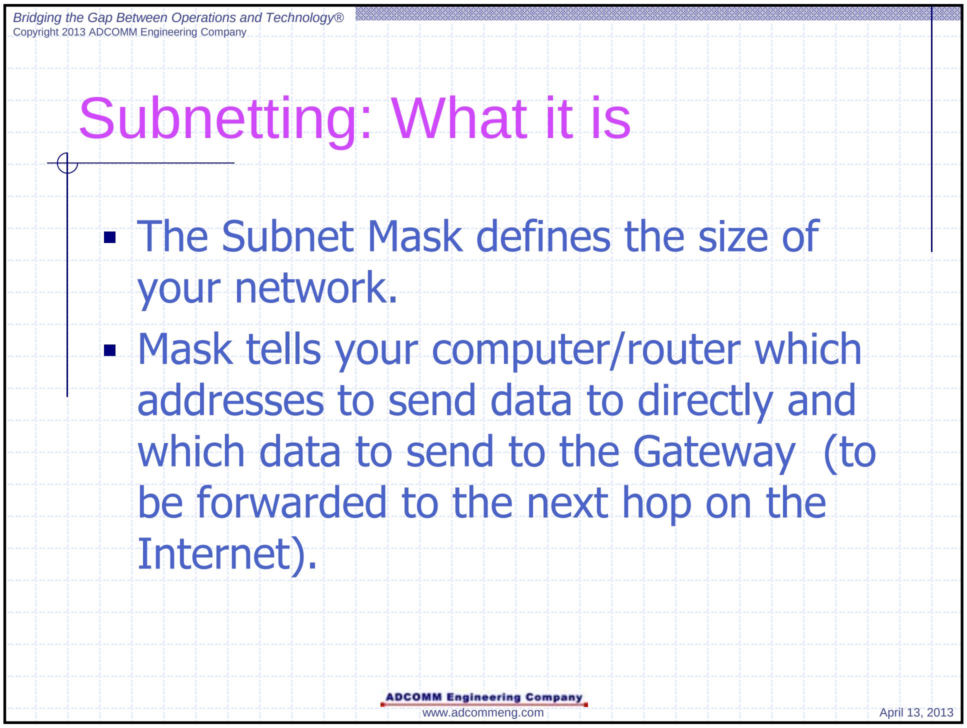


Bridging the Gap Between Operations and Technology®

Why Subnet?

ADCOMM Engineering Company
www.adcommeng.com

April 13, 2013



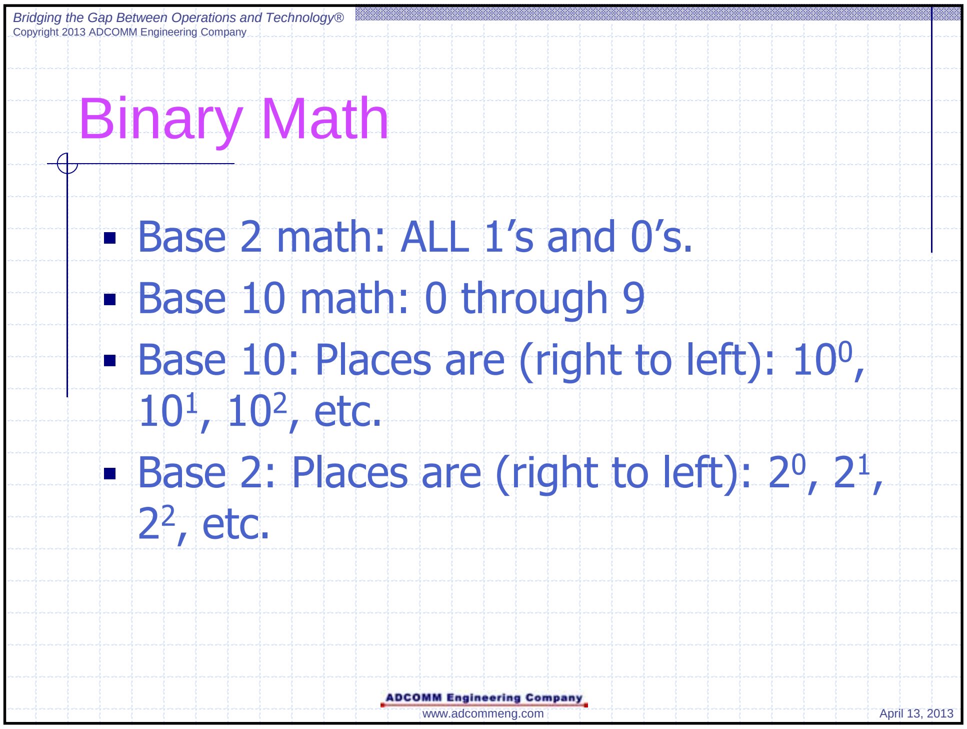
Bridging the Gap Between Operations and Technology®

Subnetting: What it is

- The Subnet Mask defines the size of your network.
- Mask tells your computer/router which addresses to send data to directly and which data to send to the Gateway (to be forwarded to the next hop on the Internet).

ADCOMM Engineering Company
www.adcommeng.com

April 13, 2013

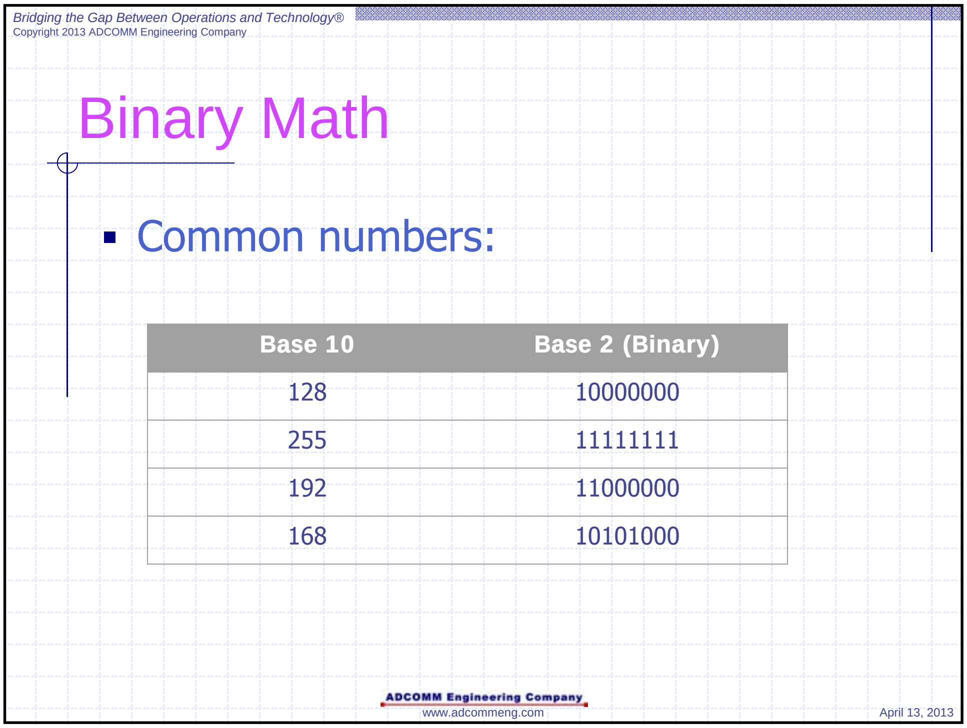


Bridging the Gap Between Operations and Technology®

Binary Math

- Base 2 math: ALL 1's and 0's.
- Base 10 math: 0 through 9
- Base 10: Places are (right to left): 10^0, 10^1, 10^2, etc.
- Base 2: Places are (right to left): 2^0, 2^1, 2^2, etc.

ADCOMM Engineering Company
www.adcommeng.com
April 13, 2013



Bridging the Gap Between Operations and Technology®

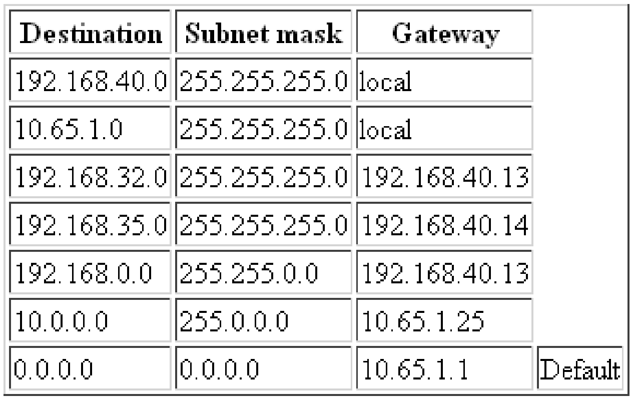
Binary Math

- Common numbers:

Base 10	Base 2 (Binary)
128	10000000
255	11111111
192	11000000
168	10101000

ADCOMM Engineering Company
www.adcommeng.com
April 13, 2013

Routing Table



Destination	Subnet mask	Gateway	
192.168.40.0	255.255.255.0	local	
10.65.1.0	255.255.255.0	local	
192.168.32.0	255.255.255.0	192.168.40.13	
192.168.35.0	255.255.255.0	192.168.40.14	
192.168.0.0	255.255.0.0	192.168.40.13	
10.0.0.0	255.0.0.0	10.65.1.25	
0.0.0.0	0.0.0.0	10.65.1.1	Default

Subnetting

- By comparing a subnet mask with an IP address, systems can determine which portion of the IP address relates to the network, and which portion relates to the host.
- Logical AND

	0	1
0	0	0
1	0	1

Subnet Mask

255.255.255.0 11111111.11111111.11111111.00000000

192.168.40.12 **11000000.10101000.00101000.00000000**

192.168.40.0

	0	1
0	0	0
1	0	1

Practical IP

- Broken? Do this:
  - Check IP addresses on end & intermediate devices
  - Check subnet masking
- Tools:
  - http://www.subnet-calculator.com/
  - http://www.tcpipguide.com/
  - Netstat –r command
  - Router print

Security

- Firewalls
- Encryption
  - Data and transport
- IPSec
- Physical security
- Administrative controls

IP Exploits

- "Spoofing"
- MITM attacks
- DoS Attacks
  - Ping attacks
    - Smurf/Fraggle (ICMP Echo)
  - DDoS delivery methods
- DNS oriented attacks
- ICMP tunneling

Security Resources

- "Security Now" podcast, Steve Gibson & Leo Laporte
- Schneier on Security: http://www.schneier.com
- Dark Reading

  http://www.darkreading.com
- The TCP/IP Guide

  http://www.tcpipguide.com/

Questions?

ADCOMM Engineering Co
Dave Magnenat, PMP
D.magnenat@adcomm911.com
360-377-4657

Bridging the Gap Between Operations and Technology®

Wireless Local Area Networks

What you need to know

Communications Academy 2013

Scott Peabody, PE

ADCOMM Engineering Company

www.adcommeng.com

4/13/13

Bridging the Gap Between Operations and Technology®

WLAN: What you need to know

ADCOMM Engineering Company

www.adcommeng.com

4/13/13

Bridging the Gap Between Operations and Technology®

Pop Quiz

How many WiFi standards are there?

a. One : 802.11-2012
b. Three: 802.11b/g/n
c. Four: 802.11a/b/g/n
d. Twenty eight: 802.11a/b/c/d/e/g/h/i/j/k/m/n/p/r/s/u/w/x/y/z/aa/ac/ad/ae/af/ah/ai

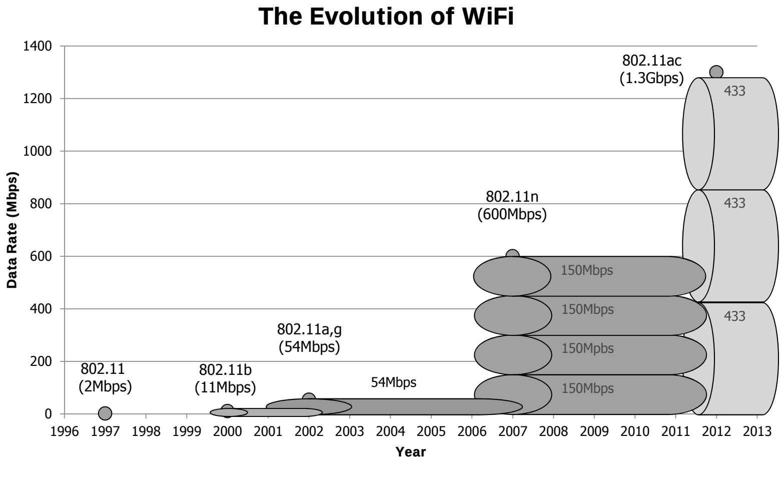
a. There is only one official standard 802.11-2012. It incorporated all approved amendments. The term standard is commonly used for the amendments which are designated by lower case letters.

ADCOMM Engineering Company
www.adcommeng.com

4/13/13

Bridging the Gap Between Operations and Technology®

WiFi Timeline



The Evolution of WiFi

ADCOMM Engineering Company
www.adcommeng.com

4/13/13

Bridging the Gap Between Operations and Technology®

How did they get more speed?

2.4 GHz

- 802.11b/g
  - 20 MHz channel width
  - 3 non-overlapping channels
  - 802.11b: 11 Mbps
  - 802.11g: 54 Mbps

5.8 GHz

- 802.11a
  - 20 MHz channel width
  - 20 non-overlapping channels
  - More bits per Hertz
  - 802.11a: 54 Mbps

2.4 and 5.8 GHz

- 802.11n
  - 20 or 40 MHz channels
  - Still more bits per Hertz
  - Up to "4 x 4" MIMO

5.8 GHz

- 802.11ac
  - 20, 40, 80 or 160 MHz chs.
  - Many more bits per Hertz
  - Up to "8 x 8" MIMO

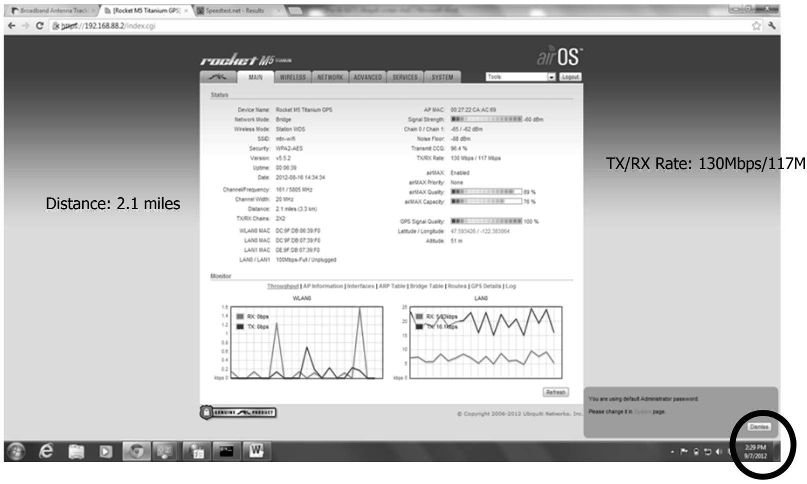
Bridging the Gap Between Operations and Technology®

What is MIMO?

MIMO: Multiple Input Multiple Output

- 802.11n and 802.11ac can simultaneously use multiple antennas
  - Space-Time Block Coding (STBC): Sends outgoing data redundantly through multiple antennas
  - Spatial Multiplexing (SM): Split outgoing data into multiple streams transmitted through multiple antennas
  - Transmit Beamforming (TxBF): Steers an outgoing stream toward the receiver to improve received signal strength

Actual Field Results



Status

Device Name: Rocket M5 Titanium GPS
Network Mode: Bridge
Wireless Mode: Station WDS
SSID: mtn-wifi
Security: WPA2-AES
Version: v5.5.2
Uptime: 00:06:39
Date: 2012-08-16 14:34:34
Channel/Frequency: 161 / 5805 MHz
Channel Width: 20 MHz
Distance: 2.1 miles (3.3 km)
TX/RX Chains: 2X2
WLAN0 MAC: DC:9F:DB:06:39:F0
LAN0 MAC: DC:9F:DB:07:39:F0
LAN1 MAC: DE:9F:DB:07:39:F0
LAN0 / LAN1: 100Mbps-Full / Unplugged

AP MAC: 00:27:22:CA:AC:69
Signal Strength: -60 dBm
Chain 0 / Chain 1: -65 / -62 dBm
Noise Floor: -88 dBm
Transmit CCQ: 96.4 %
TX/RX Rate: 130 Mbps / 117 Mbps
airMAX: Enabled
airMAX Priority: None
airMAX Quality: 89 %
airMAX Capacity: 76 %
GPS Signal Quality: 100 %
Latitude / Longitude: 47.593426 / -122.383064
Altitude: 51 m

Monitor

Throughput | AP Information | Interfaces | ARP Table | Bridge Table | Routes | GPS Details | Log

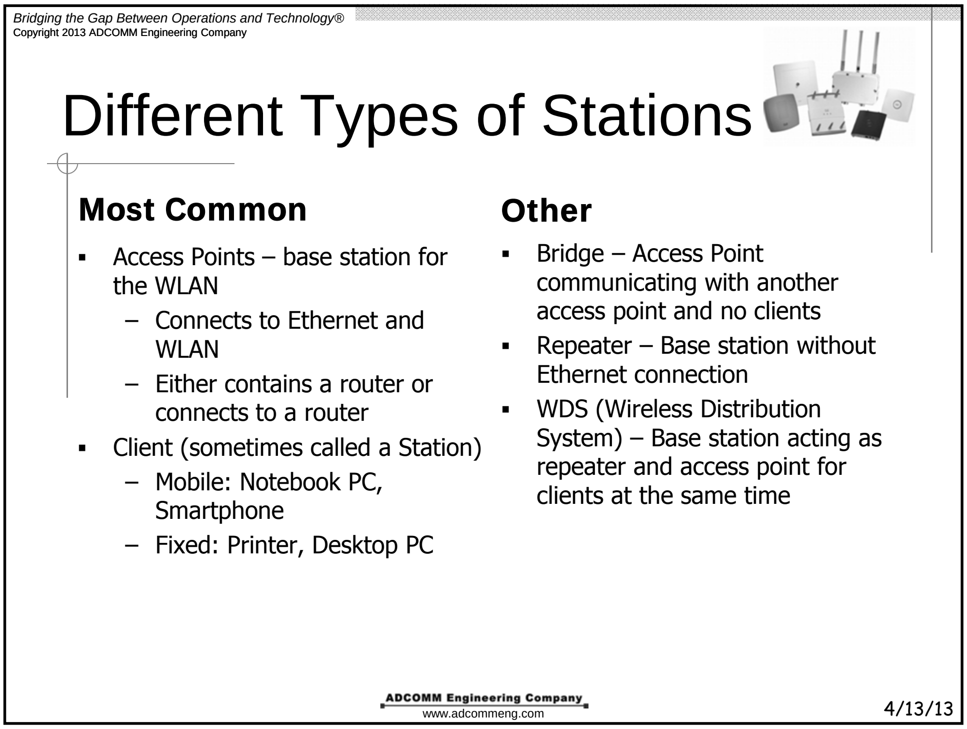
You are using default Administrator password. Please change it in System page.

Distance: 2.1 miles

TX/RX Rate: 130Mbps/117Mbps

Choices, Choices, Choices

- Different types of Stations
- Different sources of power
- Different antennas
- Many vendors



Bridging the Gap Between Operations and Technology®

Different Types of Stations

Most Common

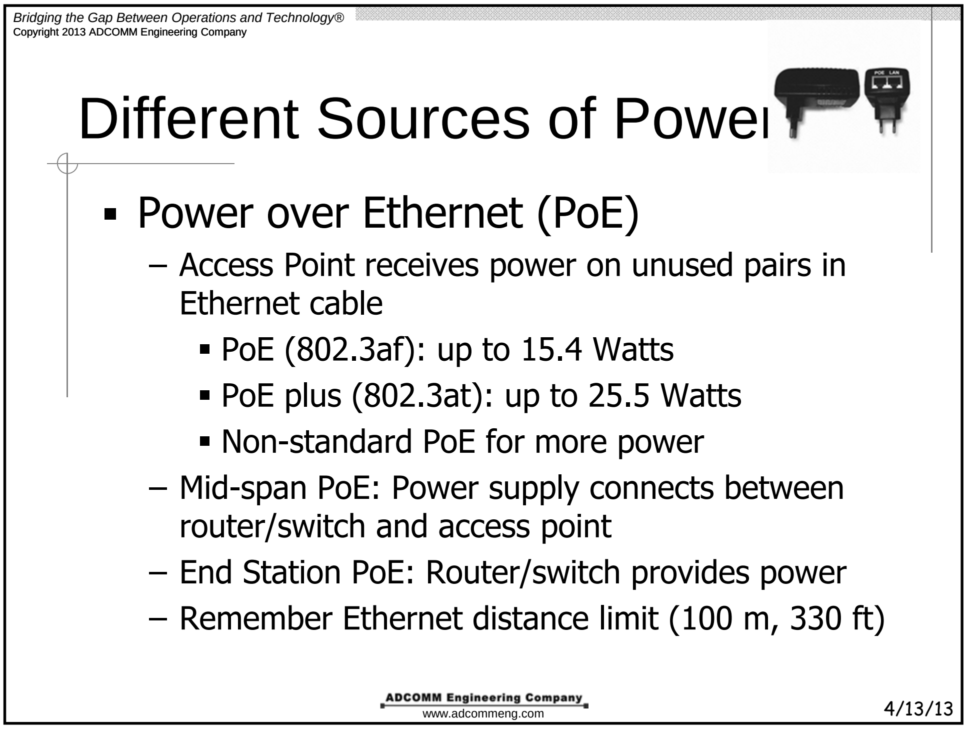
- Access Points – base station for the WLAN
  - Connects to Ethernet and WLAN
  - Either contains a router or connects to a router
- Client (sometimes called a Station)
  - Mobile: Notebook PC, Smartphone
  - Fixed: Printer, Desktop PC

Other

- Bridge – Access Point communicating with another access point and no clients
- Repeater – Base station without Ethernet connection
- WDS (Wireless Distribution System) – Base station acting as repeater and access point for clients at the same time

ADCOMM Engineering Company
www.adcommeng.com

4/13/13



Bridging the Gap Between Operations and Technology®

Different Sources of Power

- Power over Ethernet (PoE)
  - Access Point receives power on unused pairs in Ethernet cable
    - PoE (802.3af): up to 15.4 Watts
    - PoE plus (802.3at): up to 25.5 Watts
    - Non-standard PoE for more power
  - Mid-span PoE: Power supply connects between router/switch and access point
  - End Station PoE: Router/switch provides power
  - Remember Ethernet distance limit (100 m, 330 ft)

ADCOMM Engineering Company
www.adcommeng.com

4/13/13

Bridging the Gap Between Operations and Technology®

Different Types of Antennas

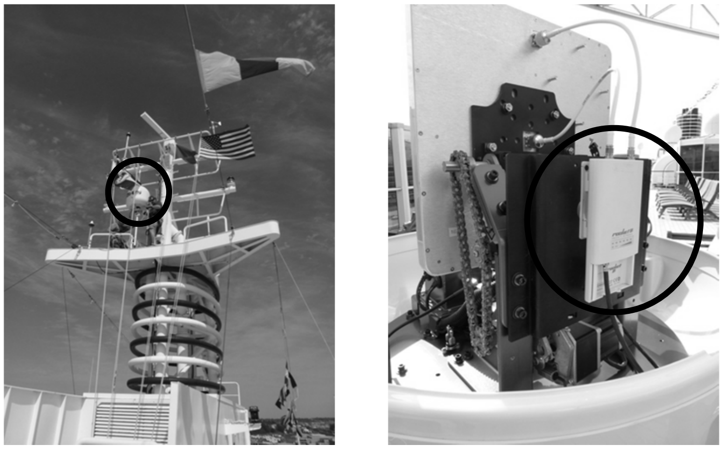
- Omnidirectional: lower gain, 360° pattern
- Directional sector: higher gain, 90° or 120° pattern
- Directional dish: highest gain, narrow beam
- Beamforming array: dynamic pattern
- Tracking antenna: directional antenna with a GPS based controller and positioner

ADCOMM Engineering Company
www.adcommeng.com

4/13/13

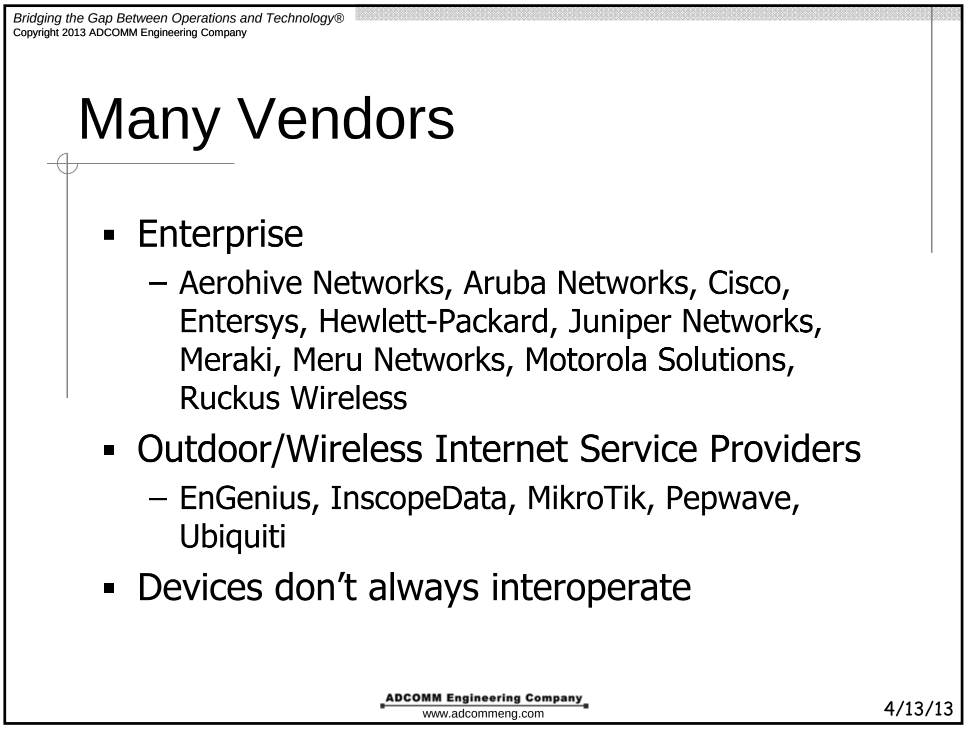
Bridging the Gap Between Operations and Technology®

Tracking Antenna and Radio



ADCOMM Engineering Company
www.adcommeng.com

4/13/13



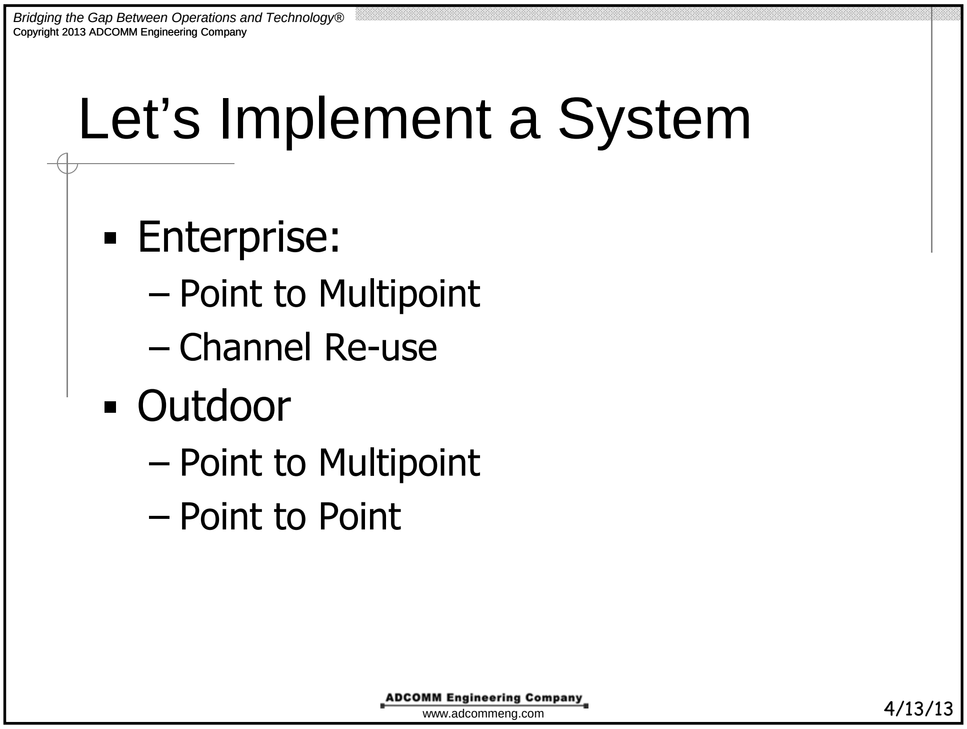
Bridging the Gap Between Operations and Technology®

Many Vendors

- Enterprise
  - Aerohive Networks, Aruba Networks, Cisco, Entersys, Hewlett-Packard, Juniper Networks, Meraki, Meru Networks, Motorola Solutions, Ruckus Wireless
- Outdoor/Wireless Internet Service Providers
  - EnGenius, InscopeData, MikroTik, Pepwave, Ubiquiti
- Devices don’t always interoperate

ADCOMM Engineering Company
www.adcommeng.com

4/13/13



Bridging the Gap Between Operations and Technology®

Let’s Implement a System

- Enterprise:
  - Point to Multipoint
  - Channel Re-use
- Outdoor
  - Point to Multipoint
  - Point to Point

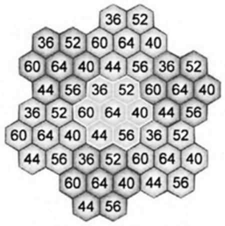
ADCOMM Engineering Company
www.adcommeng.com

4/13/13

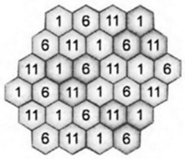
Bridging the Gap Between Operations and Technology®

Enterprise

- Point to Multipoint
- Many omnidirectional access points require frequency planning



7-to-1 Reuse pattern for 5GHz using 20MHz channels

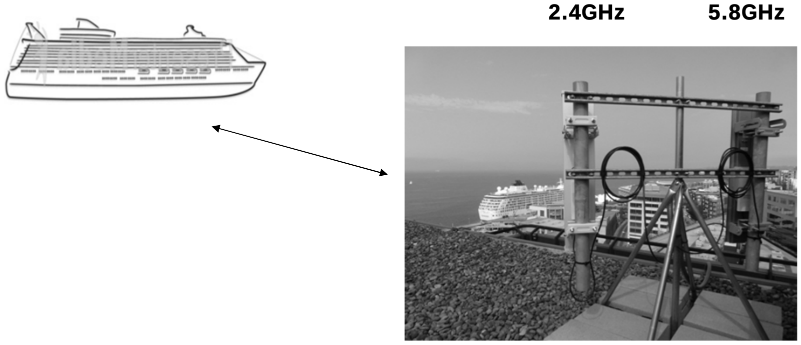


3-to-1 Reuse pattern for 2GHz using 20MHz channels

Bridging the Gap Between Operations and Technology®

Outdoor Point to Multipoint

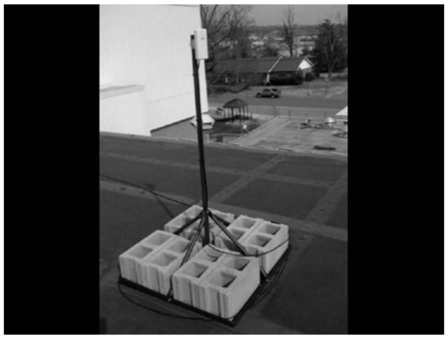
Directional Access Points
2.4GHz 5.8GHz



Bridging the Gap Between Operations and Technology®

Outdoor Point to Point

- Roof mount
- Small inexpensive radio and antenna unit



Bridging the Gap Between Operations and Technology®

WLAN: Another Threat to Security

- Security Measures
  - – Hide SSID
  - – MAC ID filtering
  - – Static ip addressing
- 802.11 Encryption

WEP (Wireless Encryption Protocol)	Obsolete, don't use it
WPA (WiFi Protected Access)	Disables speeds above 54Mbps in 802.11n
WPA2 (WPA version 2)	Recommended

WPA and WPA2 have two modes:
- Personal – Requires Pre-Shared Key (PSK)
- Enterprise – Requires Radius Server

Questions?

Thank you!

Scott Peabody, PE
s.peabody@adcomm911.com
425-766-6314
www.adcommeng.com

Bridging the Gap Between Operations and Technology®

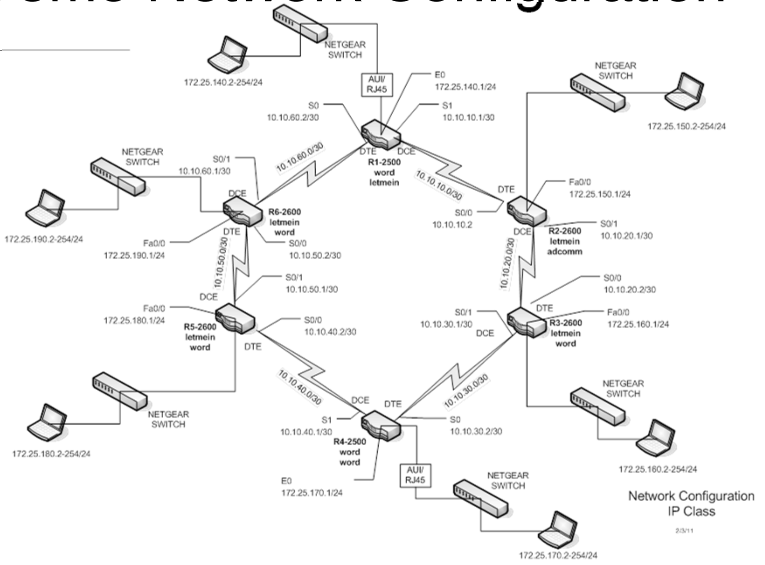
Hands-On IP for Radio Technicians

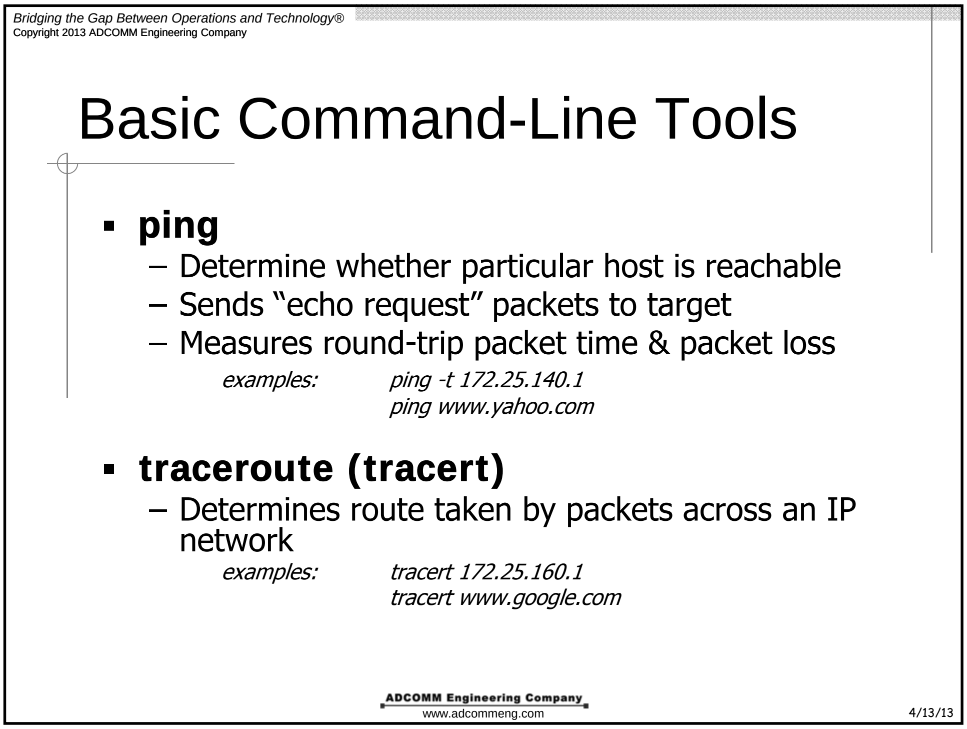
Network Troubleshooting

Communications Academy 2013
Joe Blaschka Jr., PE

Bridging the Gap Between Operations and Technology®

Demo Network Configuration





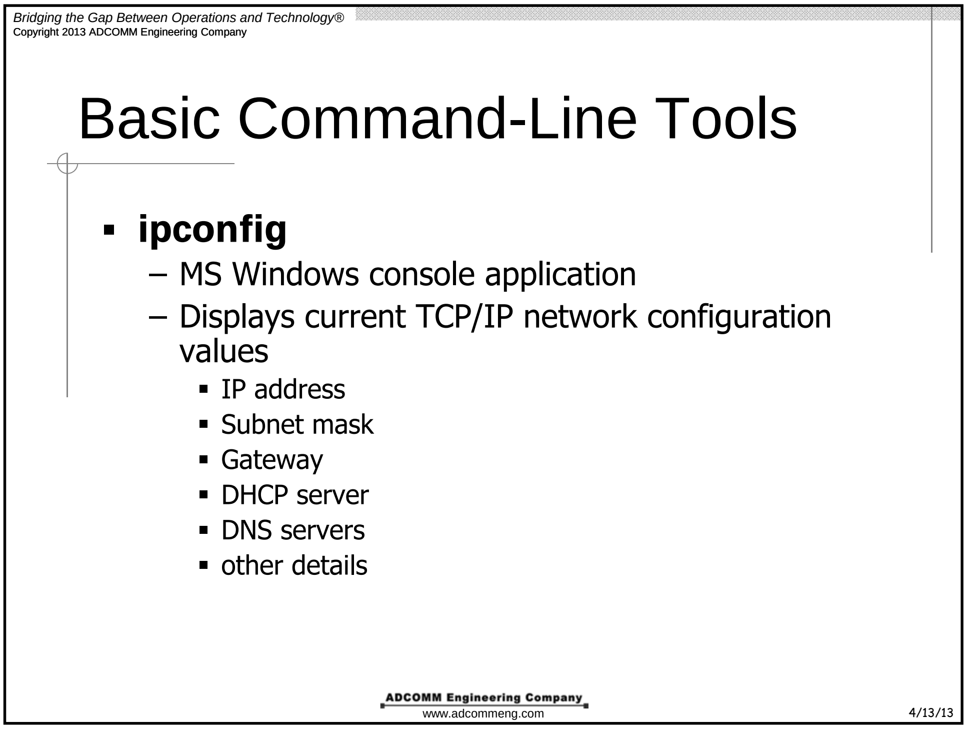
Basic Command-Line Tools

- **ping**
  - – Determine whether particular host is reachable
  - – Sends "echo request" packets to target
  - – Measures round-trip packet time & packet loss

examples: *ping -t 172.25.140.1*
ping www.yahoo.com

- **traceroute (tracert)**
  - – Determines route taken by packets across an IP network

examples: *tracert 172.25.160.1*
tracert www.google.com



Basic Command-Line Tools

- **ipconfig**
  - – MS Windows console application
  - – Displays current TCP/IP network configuration values
    - IP address
    - Subnet mask
    - Gateway
    - DHCP server
    - DNS servers
    - other details

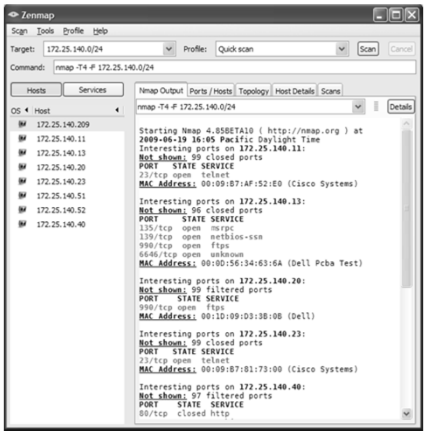
Basic Command-Line Tools

- **telnet**
  - Interactive remote login tool
  - Generally used to access a command line interface on a remote host (or device)
  - Default TCP port 23

    example: *telnet 172.25.140.50*
- **netstat -r**
  - Display PC routing table

Windows Tools

- **NMAP/Zenmap**
  - "Network Mapper"
  - Network exploration tool
  - Identifies Hosts & Running Services
  - TCP/UDP port scanner
  - NMAP: command line
  - Zenmap: GUI



Target: 172.25.140.0/24

Profile: Quick scan

Command: nmap -T4 -F 172.25.140.0/24

172.25.140.209
172.25.140.11
172.25.140.13
172.25.140.20
172.25.140.23
172.25.140.51
172.25.140.52
172.25.140.40

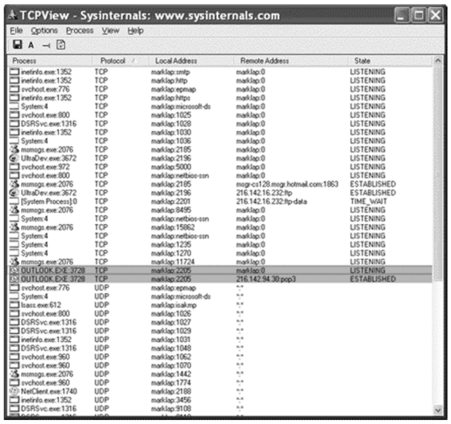
nmap -T4 -F 172.25.140.0/24

```
Starting Nmap 4.85BETA10 ( http://nmap.org ) at
2009-06-19 16:05 Pacific Daylight Time
Interesting ports on 172.25.140.11:
Not shown: 99 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:09:B7:AF:52:E0 (Cisco Systems)

Interesting ports on 172.25.140.13:
Not shown: 96 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
990/tcp  open  ftps
6646/tcp open  unknown
MAC Address: 00:0D:56:34:63:6A (Dell Pcba Test)

Interesting ports on 172.25.140.20:
Not shown: 99 filtered ports
PORT    STATE SERVICE
990/tcp open  ftps
MAC Address: 00:1D:09:D3:3B:0B (Dell)

Interesting ports on 172.25.140.23:
Not shown: 99 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:09:B7:81:73:00 (Cisco Systems)

Interesting ports on 172.25.140.40:
Not shown: 97 filtered ports
PORT    STATE  SERVICE
80/tcp  closed http
```

http://nmap.org

Windows Tools

- **TCPView**
  - Lists all TCP & UDP port endpoints on a PC
  - Similar to *netstat* command in Unix and Windows



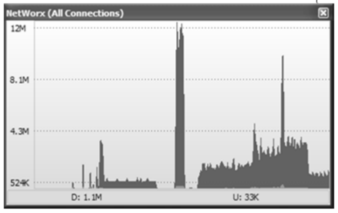
Process	Protocol	Local Address	Remote Address	State
inetinfo.exe:1352	TCP	marklap:smtp	marklap:0	LISTENING
inetinfo.exe:1352	TCP	marklap:http	marklap:0	LISTENING
svchost.exe:776	TCP	marklap:epmap	marklap:0	LISTENING
inetinfo.exe:1352	TCP	marklap:https	marklap:0	LISTENING
System:4	TCP	marklap:microsoft-ds	marklap:0	LISTENING
svchost.exe:800	TCP	marklap:1025	marklap:0	LISTENING
DSRSvc.exe:1316	TCP	marklap:1028	marklap:0	LISTENING
inetinfo.exe:1352	TCP	marklap:1030	marklap:0	LISTENING
System:4	TCP	marklap:1036	marklap:0	LISTENING
msmsgs.exe:2076	TCP	marklap:2185	marklap:0	LISTENING
UltraDev.exe:3672	TCP	marklap:2196	marklap:0	LISTENING
svchost.exe:972	TCP	marklap:5000	marklap:0	LISTENING
svchost.exe:800	TCP	marklap:netbios-ssn	marklap:0	LISTENING
msmsgs.exe:2076	TCP	marklap:2185	msgr-cs128.msgr.hotmail.com:1863	ESTABLISHED
UltraDev.exe:3672	TCP	marklap:2196	216.142.16.232:ftp	ESTABLISHED
[System Process]:0	TCP	marklap:2201	216.142.16.232:ftp-data	TIME_WAIT
msmsgs.exe:2076	TCP	marklap:8495	marklap:0	LISTENING
System:4	TCP	marklap:netbios-ssn	marklap:0	LISTENING
msmsgs.exe:2076	TCP	marklap:15862	marklap:0	LISTENING
System:4	TCP	marklap:netbios-ssn	marklap:0	LISTENING
System:4	TCP	marklap:1235	marklap:0	LISTENING
System:4	TCP	marklap:1270	marklap:0	LISTENING
msmsgs.exe:2076	TCP	marklap:11724	marklap:0	LISTENING
OUTLOOK.EXE:3728	TCP	marklap:2205	marklap:0	LISTENING
OUTLOOK.EXE:3728	TCP	marklap:2205	216.142.94.30:pop3	ESTABLISHED
svchost.exe:776	UDP	marklap:epmap	*:*	
System:4	UDP	marklap:microsoft-ds	*:*	
lsass.exe:612	UDP	marklap:isakmp	*:*	
svchost.exe:800	UDP	marklap:1026	*:*	
DSRSvc.exe:1316	UDP	marklap:1027	*:*	
DSRSvc.exe:1316	UDP	marklap:1029	*:*	
inetinfo.exe:1352	UDP	marklap:1031	*:*	
DSRSvc.exe:1316	UDP	marklap:1048	*:*	
svchost.exe:960	UDP	marklap:1062	*:*	
svchost.exe:960	UDP	marklap:1070	*:*	
msmsgs.exe:2076	UDP	marklap:1442	*:*	
svchost.exe:960	UDP	marklap:1774	*:*	
NetClient.exe:1740	UDP	marklap:2188	*:*	
inetinfo.exe:1352	UDP	marklap:3456	*:*	
DSRSvc.exe:1316	UDP	marklap:9108	*:*	

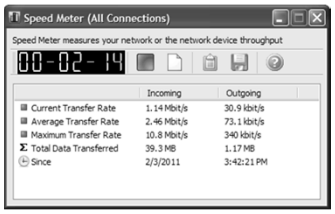
http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx

---

Windows Tools

- **Networx**
  - Live monitoring of incoming & outgoing TCP/IP bandwidth
  - Also built-in ping, traceroute, netstat, and other advanced features
  - Free MS Windows application
  - See also: Windows 8/7/Vista *Resource Monitor*





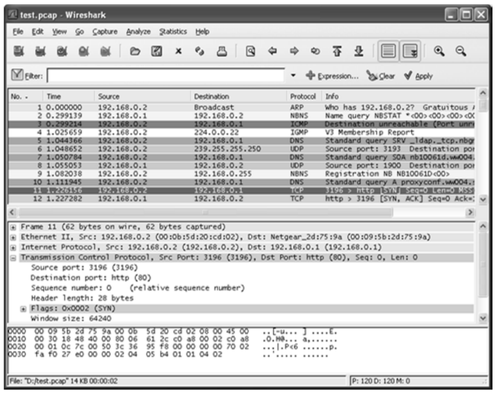
Speed Meter measures your network or the network device throughput

	Incoming	Outgoing
Current Transfer Rate	1.14 Mbit/s	30.9 kbit/s
Average Transfer Rate	2.46 Mbit/s	73.1 kbit/s
Maximum Transfer Rate	10.8 Mbit/s	340 kbit/s
Σ Total Data Transferred	39.3 MB	1.17 MB
Since	2/3/2011	3:42:21 PM

http://www.softperfect.com/products/networx/

Advanced Tools

- **Wireshark**
  - "Deep packet inspection"
  - Network protocol analyzer

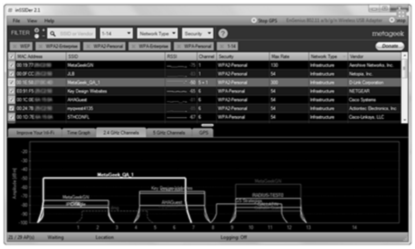

test.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

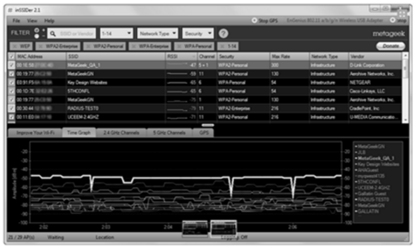
```
No. .  Time        Source         Destination       Protocol  Info
     1 0.000000    192.168.0.2    Broadcast         ARP       Who has 192.168.0.2?  Gratuitous 
     2 0.299139    192.168.0.1    192.168.0.2       NBNS      Name query NBSTAT *<00><00><00><0
     3 0.299214    192.168.0.2    192.168.0.1       ICMP      Destination unreachable (Port unr
     4 1.025659    192.168.0.2    224.0.0.22        IGMP      V3 Membership Report
     5 1.044366    192.168.0.2    192.168.0.1       DNS       Standard query SRV _ldap._tcp.nbg
     6 1.048652    192.168.0.2    239.255.255.250   UDP       Source port: 3193  Destination po
     7 1.050784    192.168.0.2    192.168.0.1       DNS       Standard query SOA nb10061d.ww004.
     8 1.055053    192.168.0.1    192.168.0.2       UDP       Source port: 1900  Destination po
     9 1.082038    192.168.0.2    192.168.0.255     NBNS      Registration NB NB10061D<00>
    10 1.111945    192.168.0.2    192.168.0.1       DNS       Standard query A proxyconf.ww004.
    11 1.226156    192.168.0.2    192.168.0.1       TCP       3196 > http [SYN] Seq=0 Len=0 MSS
    12 1.227282    192.168.0.1    192.168.0.2       TCP       http > 3196 [SYN, ACK] Seq=0 Ack=

⊞ Frame 11 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊟ Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
    Source port: 3196 (3196)
    Destination port: http (80)
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x0002 (SYN)
    Window size: 64240

0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......

File: "D:/test.pcap" 14 KB 00:00:02                    P: 120 D: 120 M: 0
```

http://www.wireshark.org

Wireless Tools

- **inSSIDer**
  - Wireless network "sniffer"

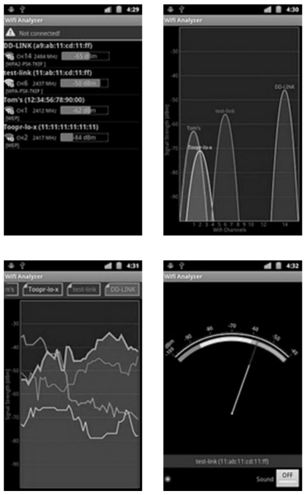




http://www.metageek.net/products/inssider/

Wireless Tools

- Mobile Apps
  - Android **WiFi Analyzer**
    - Graphical or tabular display of Wi-Fi networks in range
    - Shows signal strength vs channel or time
    - Similar functionality as inSSIDer but for mobile phone
    - Not available for iOS devices (Apple iPhone, iPad)



http://a.farproc.com/wifi-analyzer

https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer

---

Questions?

- Thank you!

ADCOMM Engineering Co.
adcomm@adcomm911.com
(425) 489-0125
www.adcommeng.com